# User Guide

## Lumension Endpoint Management and Security Suite 7.1

Lumension
IT Secured. Success Optimized.

# Notices

### Version Information

Lumension Endpoint Management and Security Suite User Guide - Lumension Endpoint Management and Security Suite Version 7.1 - Released: April 2011

Document Number: 02_201_7.1_111021147

### Copyright Information

Lumension
8660 East Hartford Drive, Suite 300
Scottsdale, AZ 85255
Phone: +1 888.725.7828
Fax: +1 480.970.6323
E-mail: *info@lumension.com*

**Copyright© 1999-2011 Lumension Security, Inc.; all rights reserved.** Some or all modules, features, or components of this intellectual property are protected by one or more of U.S. Patent Nos. 6,990,660, 7,278,158, 7,487,495, and 7,823,147; other patents are pending and other non-U.S. patents may apply. This manual, as well as the software described in it, is furnished under license. No part of this manual may be reproduced, stored in a retrieval system, or transmitted in any form – electronic, mechanical, recording, or otherwise – except as permitted by such license.

**LIMITATION OF LIABILITY/DISCLAIMER OF WARRANTY:** LUMENSION SECURITY, INC. (LUMENSION) MAKES NO REPRESENTATIONS OR WARRANTIES WITH REGARD TO THE ACCURACY OR COMPLETENESS OF THE INFORMATION PROVIDED IN THIS MANUAL. LUMENSION RESERVES THE RIGHT TO MAKE CHANGES TO THE INFORMATION DESCRIBED IN THIS MANUAL AT ANY TIME WITHOUT NOTICE AND WITHOUT OBLIGATION TO NOTIFY ANY PERSON OF SUCH CHANGES. THE INFORMATION PROVIDED IN THIS MANUAL IS PROVIDED “AS IS” AND WITHOUT WARRANTY OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE INFORMATION PROVIDED IN THIS MANUAL IS NOT GUARANTEED OR WARRANTED TO PRODUCE ANY PARTICULAR RESULT, AND THE ADVICE AND STRATEGIES CONTAINED MAY NOT BE SUITABLE FOR EVERY ORGANIZATION. NO WARRANTY MAY BE CREATED OR EXTENDED WITH RESPECT TO THIS MANUAL BY SALES REPRESENTATIVES OR WRITTEN SALES MATERIALS. LUMENSION SHALL NOT BE LIABLE TO ANY PERSON WHATSOEVER FOR ANY LOSS OF PROFIT OR DATA OR ANY OTHER DAMAGES ARISING FROM THE USE OF THIS MANUAL, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

## Trademark Information

Lumension®, *Lumension*® Endpoint Management and Security Suite, *Lumension*® Endpoint Management Platform, *Lumension*® Patch and Remediation, *Lumension*® Enterprise Reporting, *Lumension*® Security Configuration Management, *Lumension*® Content Wizard, *Lumension*® Risk Manager, *Lumension*® AntiVirus, *Lumension*® Wake on LAN, *Lumension*® Power Management, *Lumension*® Remote Management, *Lumension*® Scan™, *Lumension*® Security Configuration Management, *Lumension*® Application Control, *Lumension*® Device Control, *Lumension*® Endpoint Security, *Lumension*® Intelligent Whitelisting, PatchLink®, PatchLink® Update™, their associated logos, and all other Lumension trademarks and trade names used here are the property of Lumension Security, Inc. or its affiliates in the U.S. and other countries.

RSA Secured® is a registered trademark of RSA Security Inc.

Apache is a trademark of the Apache Software Foundation.

In addition, any other companies' names, trade names, trademarks, and products mentioned in this document may be either registered trademarks or trademarks of their respective owners.

## Feedback

Your feedback lets us know if we are meeting your documentation needs. E-mail the Lumension Technical Publications department at *techpubs@lumension.com* to tell us what you like best, what you like least, and to report any inaccuracies.

# Table of Contents

**Preface: About This Document....17**
Typographical Conventions....17
Contacting Lumension....18

**Chapter 1: Lumension Endpoint Management and Security Suite Overview....19**
The Lumension Endpoint Management and Security Suite Components....20
Explaining Module Subcomponents....21
The Lumension Endpoint Management and Security Suite Server/Client Relationship....21
Supported Agent Operating Systems....22
Recommended Agent Configuration....23
Agent Supported Locales....25
Getting Started with Lumension Endpoint Management and Security Suite....25

**Chapter 2: Using Lumension Endpoint Management and Security Suite....27**
Supported Browsers....27
Logging In to Lumension Endpoint Management and Security Suite....27
Logging Out of Lumension Endpoint Management and Security Suite....28
Common Functions within Lumension Endpoint Management and Security Suite....29
Common Conventions....30
Toolbars....31
List Pages....31
The Options Menu....31
Filters....32
Group By....35
Expanding and Collapsing Structures....36
Advancing Through Pages....36
Help....37
Exporting Data....37
The Home Page....39
The Lumension Endpoint Management and Security Suite Header....39
The Navigation Menu....40
The Dashboard....42
Dashboard Setting and Behavior Icons....48
Previewing and Printing the Dashboard....49

Editing the Dashboard ..... 49
The System Alert Pane ..... 50
License Expiration ..... 52

**Chapter 3: Configuring Default Behavior ..... 53**

The Subscription Updates Page ..... 53
Viewing the Subscription Updates Page ..... 54
Subscription Updates Page Toolbar ..... 54
Subscription Service Information ..... 55
Subscription Service History ..... 55
The Subscription Service Configuration Dialog ..... 56
Working with Subscription Updates ..... 60
Replicating ..... 60
Editing the Communication Interval ..... 60
Configuring the Service Tab ..... 60
Restarting the Subscription Service ..... 62
The Email Notifications Page ..... 62
Viewing the Email Notifications Page ..... 63
Email Notification Page Buttons ..... 63
The Email Notifications Table ..... 64
Alert Settings ..... 65
RSS Feed ..... 66
Working with Email Notifications ..... 67
Defining Alert Settings ..... 67
Creating Email Notification Addresses ..... 68
Editing Email Notification Addresses ..... 69
Deleting Email Notification Addresses ..... 69
Exporting Email Notification Data ..... 70
Testing Email Notifications ..... 70
The Options Page ..... 70
The Options Page Buttons ..... 71
Viewing the Options Page ..... 71
The General Tab ..... 72
The Agents Tab ..... 74
Working with Options ..... 78
Configuring the General Tab ..... 79
Configuring the Agents Tab ..... 80

Exporting Option Data....83

**Chapter 4: Licensing and Support....85**

The Technical Support Page....86

Viewing the Technical Support Page....86

Technical Support Page Buttons....86

Technical Support Options....87

Server Information....88

Suite Version Information....90

Regenerating OS Packs....90

Exporting Technical Support Data....90

The Product Licensing Page....91

Viewing the Product Licensing Page....91

The Product Licensing Page Buttons....91

The Product Licensing Page List....92

Initiating Subscription License Replication Jobs....93

Exporting Product Information....93

**Chapter 5: Discovering Assets....95**

About Discovery Scan Jobs....95

The Discovery Scan Process....96

Working with Discovery Scan Jobs....97

Discovering Assets by Discovery Scan Job....97

About Agent Management Jobs....109

Working with Agent Management Jobs....110

Installing Agents by Agent Management Job....111

Uninstalling Agents by Agent Management Job....124

**Chapter 6: Reviewing Jobs and Job Results....137**

About Reviewing Jobs....137

The Job Results Page....138

Viewing the Job Results Page....138

The Scheduled Tab....139

The Scheduled Tab Toolbar....139

The Scheduled Tab List....140

The Active Tab....141

The Active Tab Toolbar....141

The Active Tab List....142

The Completed Tab....143
The Completed Tab Toolbar....143
The Completed Tab List....144
Working with Jobs....145
Discovering Assets....146
Installing Agents by Agent Management Job....146
Uninstalling Agents by Agent Management Job....146
Copying Jobs....146
Viewing Job Configurations....147
Deleting Jobs....148
Exporting Job Result Data....149
Canceling Jobs....149
Viewing a Job Log....149
Viewing Job Results....150
Pausing Jobs....151
Resuming a Paused Job....151
Merging Jobs....152
The Results Page....153
Viewing the Results Page....154
The Results Page Toolbar....154
The Results Page List....156
Working with Results....157
Viewing Endpoint Details....157
Installing Agents by Agent Management Job....158
Uninstalling Agents by Agent Management Job....158
Downloading the Agent Installer....158
Changing Endpoint Operating System Results....158
Deleting Job Endpoint Results....159
Exporting Discovery Scan Result Data....160

**Chapter 7: Using Endpoints....161**

About Endpoints....161
Viewing the Endpoints Page....161
The Endpoints Page....162
The All Tab....162
Working with the Endpoints Page....165
Installing an Agent....165

Installing Agents by Agent Management Job....165
Uninstalling Agents by Agent Management Job....165
Defining the Endpoint Agent Version....166
Downloading the Agent Installer....166
Deleting an Endpoint....167
Enabling Modules on Endpoint....168
Enabling an Endpoint....168
Disabling Modules on Endpoint....168
Disabling an Endpoint....169
The Add/Remove Modules Dialog....169
Exporting Endpoint Information....170
The Endpoint Details Page....171
Viewing the Endpoint Details Page....171
The Information Tab....172
Working with the Endpoint Details Page....179
Viewing the Agent Uninstall Password....180
Defining the Endpoint Agent Version (Endpoint Details)....181
Enabling an Endpoint....181
Disabling an Endpoint....182
Managing Endpoint Modules....182
Exporting Endpoint Information....183

**Chapter 8: Using Groups....185**

About Groups....185
The Groups Page....186
The Group Browser Directory Tree....186
Viewing Groups....188
Searching for a Group....189
The Information View....189
Information View....190
Email Notification Addresses....191
Child Groups....191
Agent Policy Sets....192
Resultant Agent Policy Set Information....192
Roles....193
Exporting Information View Data....193
The Group Membership View....194

The Group Membership View Toolbar....194
The Group Membership View List....195
Creating a Group....195
Editing Groups....196
Deleting Groups....197
Moving a Group....197
Exporting Group Membership View Data....199
The Endpoint Membership View....200
The All Tab (Groups Page)....200
Adding Endpoint Members....202
Removing Endpoint Members....203
Installing Agents by Agent Management Job....204
Uninstalling Agents by Agent Management Job....204
Downloading the Agent Installer....204
Defining the Endpoint Agent Version (Groups Page)....205
Deleting Endpoint (Groups Page)....205
Enabling or Disabling Endpoints within a Group....206
Managing Endpoint Modules (Groups Page)....206
Exporting Endpoint Membership View Data....207
The Agent Policy Sets View....207
The Agent Policy Sets View Toolbar....208
The Agent Policy Sets View List....208
Assigning an Agent Policy Set to a Group....209
Removing an Agent Policy Set from a Group....209
Creating an Agent Policy Set (Groups Page)....210
Exporting Agent Policy Set View Data....210
The Roles View....211
The Roles View Toolbar....211
The Roles View List....212
Adding a Role to a Group....212
Removing a Role from a Group....213
Creating User Roles (Roles View)....214
Exporting Roles View Data....215
The Dashboard View....215
Group Dashboard Widgets....216
Widget Setting and Behavior Icons....217
Previewing and Printing the Dashboard....217

Editing the Dashboard ..... 217
The Settings View ..... 218
Editing Group Settings ..... 218
Exporting Settings View Data ..... 222

**Chapter 9: Managing Agent Policy Sets ..... 223**
The Agent Policy Sets Page ..... 223
About Agent Policies and Agent Policy Sets ..... 223
Viewing the Agent Policy Sets Page ..... 224
The Agent Policy Sets Page Toolbar ..... 224
The Agent Policy Sets Page List ..... 225
Working with Agent Policy Sets ..... 226
Creating an Agent Policy Set ..... 226
Editing an Agent Policy Set ..... 227
Deleting an Agent Policy Set ..... 228
Defining the Global Uninstall Password ..... 229
Defining Agent Policy Logging Levels ..... 230
Defining Agent Policy Inheritance Rules ..... 232
Defining Agent Policy Conflict Resolution ..... 232
Exporting Agent Policy Set Data ..... 233
Assigning an Agent Policy Set to a Group ..... 233
Removing an Agent Policy Set from a Group ..... 234

**Chapter 10: Reporting ..... 235**
About Reports ..... 235
The All Reports Page ..... 236
Viewing the All Reports Page ..... 236
The Display List ..... 237
The Report Description ..... 238
Generating a Report ..... 238
Working with HTML Reports ..... 239
Displaying Time and Date in HTML Reports ..... 239
Exporting HTML Reports ..... 239
Previewing and Printing HTML Reports ..... 240
Working with PDF Reports ..... 240
Available Reports ..... 240
Available Core Reports ..... 240

**Chapter 11: Managing Lumension EMSS Users and Roles ..... 249**
The Users and Roles Page ..... 249
Viewing the Users and Roles Page ..... 250
Defining User Access ..... 250
The Users Tab ..... 251
Defining Users ..... 251
The Users Tab Toolbar ..... 252
The Users Tab List ..... 252
Working with Users ..... 253
Creating New Lumension EMSS Users ..... 253
Adding Existing Windows Users to Lumension EMSS ..... 255
Editing Lumension EMSS Users ..... 257
Removing Lumension EMSS Users ..... 258
Deleting Lumension EMSS Users ..... 259
Changing a User Password ..... 259
Changing Your Password ..... 260
Exporting User Data ..... 261
The Roles Tab ..... 262
Defining Roles ..... 262
Defining Access Rights ..... 263
Defining Accessible Groups ..... 266
Defining Accessible Endpoints ..... 267
The Roles Tab Toolbar ..... 268
The Roles Tab List ..... 269
Working with Roles ..... 269
Creating User Roles ..... 270
Editing User Roles ..... 271
Disabling User Roles ..... 273
Enabling User Roles ..... 273
Deleting User Roles ..... 273
Exporting User Role Data ..... 274

**Chapter 12: Using Lumension Installation Manager ..... 275**
Lumension Installation Manager ..... 275
Accessing Lumension Installation Manager ..... 276
Accessing Installation Manager Via Lumension Endpoint Management and Security Suite ..... 276
Accessing Installation Manager Via Windows ..... 277

Logging Out ... 277
The Navigation Menu ... 278
The Home Page ... 279
The New/Update Components Tab ... 280
The New/Update Components Tab List ... 281
The New/Update Components Tab Buttons ... 281
Working with Installs and Updates ... 282
Downloading Components ... 282
Installing or Updating Components ... 284
The Existing Components Tab ... 286
The Existing Components Tab List ... 286
The Existing Components Tab Buttons ... 287
Working with Uninstalls ... 287
Uninstalling Module Components ... 288
The Installation Log ... 289
Viewing the Installation Log ... 289
The Installation Log List ... 290
The Installation Log Buttons ... 290
The Installation Manager Technical Support Page ... 291
Viewing the Technical Support Page ... 292
Technical Support Options ... 292
Server Information ... 292
Suite Version Information ... 293
The Installation Manager Product Licensing Page ... 294
Viewing the Product Licensing Page ... 294
The Product Licensing Page Buttons ... 294
The Product Licensing Page List ... 295
Validating License Information ... 295

**Chapter 13: Using the Lumension Endpoint Management and Security Suite Agent ... 297**

Upgrading Agents on Endpoints ... 298
The Agent Control Panel ... 299
Accessing the Agent Control Panel ... 300
The Summary Panel ... 300
Agent Information ... 301
Endpoint Details ... 301
Server Details ... 302

The Proxy Server Panel ..... 302
Defining Proxy Settings ..... 303

**Appendix A: Server Reference ..... 305**
Server Security ..... 305
Server Error Pages ..... 306
WinInet Error Codes ..... 307
HTTP Status Codes ..... 307
Defining Targets Using Wildcards ..... 308
Defining Targets Within an Imported File ..... 309
Setting Up Lumension Endpoint Management and Security Suite ..... 311
Restarting the STATEngine Service ..... 313

**Appendix B: Securing Your Server ..... 315**
Secure Your Server With SSL ..... 315
Use Secure Passwords ..... 316
Disabling File and Printer Sharing ..... 316
Disabling File and Printer Sharing in Windows Server 2003 ..... 316
Disabling File and Printer Sharing in Windows Server 2008 ..... 317
Placing Your Server Behind a Firewall ..... 318
Disable Non-Critical Services ..... 318
Lock Down Unused TCP and UDP Ports ..... 318
Disabling Unused Ports in Windows Server 2003 ..... 318
Apply All Security Patches ..... 322

**Appendix C: Configuring the Server and Endpoints for Agent Management Jobs ..... 323**
Configuring the Scanning System ..... 323
Configuring Pre-Windows Vista Endpoint for Discovery ..... 324
Configuring Endpoints for Agent Management Jobs (Pre-Windows Vista) ..... 326
Configuring Post-Windows Vista Endpoints for Discovery ..... 331
Configuring Endpoints for Agent Management Jobs (Post-Windows Vista) ..... 334
Resolving Endpoint UAC Issues ..... 339
Troubleshooting Agent Management Jobs ..... 340
Disabling Password Changes ..... 341

**Appendix D: Creating a Disaster Recovery Solution ..... 343**
Preparing Your Database ..... 343
Changing the Database Recovery Model ..... 343
Creating a Manual Solution ..... 345

Creating a Database Backup....345
Restoring a Database Backup....348
Creating an Automated Solution....351
Creating a Maintenance Plan....352

**Appendix E: Installation Manager Reference....357**
Configuring Windows Firewall for Installation Manager....357
Updating Lumension Installation Manager....361

**Appendix F: Glossary....363**
Glossary....363

# Preface

## About This Document

This User Guide is a resource written for all users of Lumension Endpoint Management and Security Suite 7.1. This document defines the concepts and procedures for installing, configuring, implementing, and using Lumension Endpoint Management and Security Suite 7.1.

**Tip:** Lumension documentation is updated on a regular basis. To acquire the latest version of this or any other published document, please refer to the *Lumension Customer Portal* (*http://portal.lumension.com/*).

### Typographical Conventions

The following conventions are used throughout this documentation to help you identify various information types.

Table 1: Typographical Conventions

| Convention | Usage |
|---|---|
| **bold** | Buttons, menu items, window and screen objects. |
| ***bold italics*** | Wizard names, window names, and page names. |
| *italics* | New terms, options, and variables. |
| `MONOSPACE UPPERCASE` | Keyboard keys. |
| **`BOLD UPPERCASE`** | SQL Commands. |
| `monospace` | File names, path names, programs, executables, command syntax, and property names. |

# Contacting Lumension

**Global Headquarters**

8660 East Hartford Drive
Suite 300
Scottsdale, AZ 85255
United States of America

Phone: +1 888 725 7828
Phone: +1 480 970 1025
Fax: +1 480 970 6323

**Ireland Office**

Lumension Security Ireland Ltd.
Lyrr Building, Second Floor
Mervue Business & Technology Park
Mervue, Galway
Ireland

Phone: +353 91 44 8980
Fax: +353 91 76 6722

**Luxembourg Office**

Lumension Security SA
Atrium Business Park
Z.A Bourmicht
23, rue du Puits Romain
L-8070 Bertrange
Luxembourg

Phone: +352 265 364 11
Fax: +352 265 364 12

**Endpoint Security Technical Support**

**Phone:**
+1 877 713 8600 (US Toll Free)
+44 800 012 1869 (UK Toll Free)
+353 9142 2999 (EMEA)

**Email:**
*endpoint.support@lumension.com*

**Vulnerability Management Technical Support**

**Phone:**
+1 888 725 7828 (option 2) (US Toll Free)
+44 800 012 1869 (UK Toll Free)
+353 9142 2999 (EMEA)
+61 (02) 8223 9810 (Australia)
+852 3071 4690 (Hong Kong)
+65 6622 1078 (Singapore)

**Email:**
*patchlink.support@lumension.com (US)*
*patchlink.apac.support@lumension.com (APAC)*
*patchlink.emea.support@lumension.com (EMEA)*

**Note:** For additional contact information, please visit the *Contact Lumension* page at *http://www.lumension.com/contact-us.aspx*.

# Chapter 1

# Lumension Endpoint Management and Security Suite Overview

**In this chapter:**


- The Lumension Endpoint Management and Security Suite Components
- Explaining Module Subcomponents
- The Lumension Endpoint Management and Security Suite Server/Client Relationship
- Supported Agent Operating Systems
- Recommended Agent Configuration
- Agent Supported Locales
- Getting Started with Lumension Endpoint Management and Security Suite


Lumension Endpoint Management and Security Suite (Lumension EMSS) is an application that serves as a platform for other applications that protect your network from security risks.

These applications, called *modules*, use different approaches to protect your endpoint. For example, the Lumension Patch and Remediation module protects your network by detecting software vulnerabilities and then patching them, while the Lumension Application Control module protects your network by allowing only authorized applications to run on network endpoints. You may purchase any combination of these modules to best protect your network environment.

# The Lumension Endpoint Management and Security Suite Components

Lumension Endpoint Management and Security Suite (Lumension EMSS) consists of components. These components include *platform components* and *module components*.

| | |
|---|---|
| **Platform Components** | Platform components form the basis for Lumension EMSS module components to operate.<br>The Lumension EMSS platform components include:<br>• The Lumension Endpoint Management and Security Suite Web Console. The console is used to control Lumension Endpoint Management and Security Suite.<br>• The Lumension Endpoint Management and Security Suite Database. The database stores Lumension Endpoint Management and Security Suite values.<br>• The Lumension Installation Manager. Installation Manager is used to install module components.<br>All Lumension EMSS platform components are included in the Lumension EMSS install. |
| **Module Components** | Modules components are the individual security solutions used to prevent various types of security breaches within your network. Each module plugs in to the Lumension EMSS platform and can be purchased individually.<br>Each module prevents breaches stops security threats using a different approach. For example, Lumension Patch and Remediation stops security threats by applying vendor-created software patches.<br>You can install, upgrade, or uninstall any module you are licensed for with Lumension Installation Manager. You can manage modules regardless of purchase time. For example, you may initially purchase only the Lumension Patch and Remediation module, but later add the Application Control module.<br>For additional information about Lumension Installation Manager, refer to the following topics:<br>• *Lumension Installation Manager* on page 275<br>• *Explaining Module Subcomponents* on page 21<br>For information about purchasing additional modules, contact *Lumension Sales Support* (*patchlink.sales@lumension.com*). |

## Explaining Module Subcomponents

Each Lumension Endpoint Management and Security Suite module is composed of two subcomponents: the server component and the endpoint component.

| | |
|---|---|
| **Server Component** | This subcomponent is installed on the Lumension Endpoint Management and Security Suite server. The server component must be installed before the endpoint component. |
| **Endpoint Component** | This subcomponent is installed on endpoints hosting a Lumension Endpoint Management and Security Suite Agent. Endpoint components can be installed after the server component and agents are installed. |

## The Lumension Endpoint Management and Security Suite Server/ Client Relationship

To protect your network from security exposures, Lumension Endpoint Management and Security Suite operates using a server/client relationship.

Through communication between the server (a server with the Lumension Endpoint Management and Security Suite Server installed) and the client (an endpoint with the Lumension Endpoint Management and Security Suite Agent installed), the Lumension Endpoint Management and Security Suite system protects your network from various types of vulnerabilities.

| | |
|---|---|
| **The Lumension EMSS Server** | This software, installed on a server in the network, is the platform for all Lumension EMSS modules. It detects endpoints in your networks, collects information from managed endpoints, and sends information and commands to those managed endpoints. You can control the server from a Web-based UI, accessible from any network endpoint. With no modules installed, Lumension EMSS offers the following functionality:<br>• Asset Discovery<br>• Agent Installation<br>• Endpoint Management<br>• Basic Reporting |
| **The Lumension EMSS Agent** | This software, installed on network endpoints, collects information about the endpoint and uploads it to the Lumension EMSS Server. Through communication with the server, the agent can control various endpoint functionality. As more modules are activated, agent responsibility increases. |

## Supported Agent Operating Systems

There are multiple versions of the Lumension Endpoint Management and Security Suite (Lumension EMSS) Agent to accommodate multiple operating systems. In some cases, more than one agent version can be installed on a particular operating system.

The following table lists the Windows platforms on which the agent is supported.

Table 2: Supported Windows Operating Systems

| Operating System | Version | Edition | Data Width | Proc. Family | Software Prerequisites | Agent Version |
|---|---|---|---|---|---|---|
| Microsoft Windows XP SP2+ | 5.1 | Professional(2) | 32/64 bit | Intel | Microsoft Windows Installer 2.0+ | Lumension EMSS 7.1 Agent |
| Microsoft Windows 2003 SP1+ | 5.2 | Web<br>Standard<br>Enterprise<br>R2 | 32/64 bit | Intel | Microsoft Windows Installer 2.0+ | Lumension EMSS 7.1 Agent |
| Microsoft Windows Vista | 6.0 | Business (3)<br>Enterprise<br>Ultimate | 32/64 bit | Intel | Microsoft .NET Framework 3.0+ | Lumension EMSS 7.1 Agent |
| Microsoft Windows Server 2008 | 6.0 | Web(4)<br>Standard<br>Enterprise | 32/64 bit | Intel | Microsoft .NET Framework 3.0+ | Lumension EMSS 7.1 Agent |
| Microsoft Windows 7 | 7 | Professional<br>Enterprise<br>Ultimate | 32/64 bit | Intel | Microsoft .NET Framework 3.0+ | Lumension EMSS 7.1 Agent |
| Microsoft Windows 2008 R2 | 7 | Standard<br>Enterprise<br>Web | 64 bit | Intel | Microsoft .NET Framework 3.0+ | Lumension EMSS 7.1 Agent |

(1) The Datacenter editions of this OS family are not supported.

(2) Home, Media Center, and Tablet PC editions are not supported.

(3) Home edition is not supported.

(4) The Datacenter and Core Editions of this OS family are not supported.

The following table lists the Linux, UNIX, and Apple platforms on which the agent is supported.

Table 3: Supported Linux, UNIX, and Apple Operating Systems

| Operating System | Version | Edition | Data Width | Proc. Family | Software Prerequisites | Agent Version |
|---|---|---|---|---|---|---|
| Apple Mac OS X | 10.3<br>10.4<br>10.5<br>10.6 | All | 32/64 bit | Intel / PowerPC | Sun Java JRE 1.5.0+ | Lumension EMSS 7.0 Agent |
| HP-UX | 11.11<br>11.23<br>11.31 | All | 64 bit | PA-RISC | Sun Java JRE 1.5.0+ | Patch 7.0 Agent |
| IBM AIX | 5.3<br>6.1 | All | 32/64 bit | Power / PowerPC | Sun Java JRE 1.5.0+ | Patch 7.0 Agent |
| Novell SUSE Linux | 9<br>10 | Enterprise | 32/64 bit | Intel | Sun Java JRE 1.5.0+ | Patch 7.0 Agent |
| Red Hat Linux | 4.0<br>5.0 | Enterprise<br>AS<br>ES<br>WS | 32/64 bit | Intel | Sun Java JRE 1.5.0+ | Patch 7.0 Agent |
| Oracle Solaris | 9<br>10 | All | 32/64 bit | SPARC / Intel | Sun Java JRE 1.5.0+ | Patch 7.0 Agent |
| Oracle Linux | 4<br>5 | All | 32/64 bit | Intel | Sun Java JRE 1.5.0+ | Patch 7.0 Agent |
| CentOS Linux | 4<br>5 | All | 32/64 bit | Intel | Sun Java JRE 1.5.0+ | Patch 7.0 Agent |

## Recommended Agent Configuration

Lumension recommends configuring server-to-agent communication according to the number of managed endpoints in your network.

After installing Lumension Endpoint Management and Security Suite Server and Agents, Lumension recommends configuring agent settings according to your network size.

Lumension recommends the following settings for the Lumension EMSS Agent.

Table 4: Application Settings: Lumension EMSS Agent

| **Endpoint Count** | **>250** | **>1,000** | **>2,500** | **>5,000** | **>10,000** |
|---|---|---|---|---|---|
| Send interval (sec) | 2 | 3 | 4 | 5 | 6 |
| Receive interval (sec) | 0 | 0 | 0 | 0 | 0 |
| Timeout interval | 12 hours | 12 hours | 12 hours | 12 hours | 12 hours |
| Heartbeat interval | 30 min | 30 min | 30 min | 60 min | 90 min |

**Note:** If managing more than 10,000 endpoints, contact *Lumension Support* (*http://support.lumension.com*) for a recommended configuration.

## Agent Supported Locales

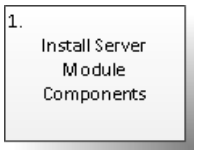
The Lumension Endpoint Management and Security Suite Agent is only supported on operating systems that use certain locales. Ensure the endpoint you are installing an agent on uses one of the listed locales.

- da-DA: Danish (Denmark)
- en-AU: English (Australia)
- en-BZ: English (Belize)
- en-CA: English (Canada)
- en-IN: English (India)
- en-IE: English (Ireland)
- en-JM: English (Jamaica)
- en-NZ: English (New Zealand)
- en-PH: English (Philippines)
- en-SG: English (Singapore)
- en-ZA: English (South Africa)
- en-GB: English (United Kingdom)
- en-US: English (United States)
- es-ES: Spanish (Spain)
- fi-FI: Finnish (Finland)
- fr-FR: French (France)
- de-DE: German (Germany)
- it-IT: Italian (Italy)
- ja-JP: Japanese (Japan)
- ko-KR: Korean (Korea)
- nl-NL: Dutch (Netherlands)
- no-NO: Norwegian - Nynorsk (Norway)
- pt-BE: Portuguese (Brazil)
- ru-RU: Russian (Russia)
- sv-SE: Swedish (Sweden)
- zh-CN / zh-CHS: Chinese (China [Simplified])
- zh-TW / zh-CHT: Chinese (Taiwan [Traditional])

## Getting Started with Lumension Endpoint Management and Security Suite

After initial installation of the Lumension Endpoint Management and Security Suite Server, you must install the Lumension Endpoint Management and Security Suite Agent on network endpoints to create an infrastructure to use Lumension Endpoint Management and Security Suite modules and their functions.

The following chart lists the tasks you should perform after installing the Lumension Endpoint Management and Security Suite Server and logging in for the first time.

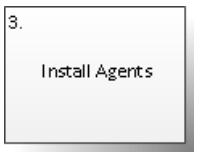



Install server modules components using *Installation Manager*. Installation Manager is a utility you can use to install module server components on Lumension EMSS that you are licensed for.

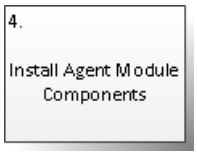
**Note:** By default, all modules you are licensed for are installed during the initial Lumension EMSS Server installation.

You can purchase and install new modules at any time. For additional information on installing modules, refer to *Installing or Updating Components* on page 284.

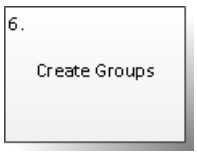
Complete a *Discovery Scan Job*. Discovery scan jobs search your network for endpoints. After completing this scan, you can select which endpoints you want to install agents on. For additional information, refer to *Discovering Assets by Discovery Scan Job* on page 97.



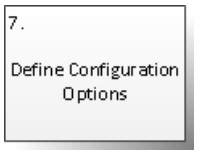

Complete an *Agent Management Job*. Agent management jobs install the Lumension Endpoint Management and Security Suite Agent on defined network endpoints. The agent communicates with the Lumension Endpoint Management and Security Suite Server to create an infrastructure for Lumension EMSS module functions. For additional information, refer to *Installing Agents by Agent Management Job* on page 111.




Install module endpoint components. To activate a module's functions on an endpoint, you must install the module's endpoint component on the endpoint's agent. For additional information, refer to *Managing Module Endpoint Components* on page 170.




Create *Groups*. Groups are collections of endpoints that you create. You can group endpoints by operating system, function, or any other method to suit your organization. After forming groups, you can manage them collectively. For additional information, refer to *Creating a Group* on page 195.




Define configuration options. These configuration options control how the Lumension EMSS Server communicate with the Lumension EMSS Agent. For additional information, refer to the following topics:

- *Configuring Default Behavior* on page 53
- *Managing Agent Policy Sets* on page 223

Define users and user roles. Users are people who have access to Lumension EMSS, and user roles define the features Lumension EMSS users have access to. For additional information, refer to *Managing Lumension EMSS Users and Roles* on page 249.

# Chapter 2

# Using Lumension Endpoint Management and Security Suite

**In this chapter:**


- Supported Browsers
- Common Functions within Lumension Endpoint Management and Security Suite
- The Home Page


Within Lumension Endpoint Management and Security Suite (Lumension EMSS), you can use a number of common functions to navigate and operate the system. After you log in, Lumension EMSS opens to the ***Home*** page.

## Supported Browsers

Lumension Endpoint Management and Security Suite is managed using a Web browser.

The following list defines the Web browsers supported byLumension Endpoint Management and Security Suite, along with other software required to use all Lumension Endpoint Management and Security Suite functions.

- Internet Information Services (IIS) 6.0 or later.
- One of the following; Microsoft Internet Explorer 7, Microsoft Internet Explorer 8, or Mozilla Firefox 3.5.x.
- Microsoft Silverlight™.

### Logging In to Lumension Endpoint Management and Security Suite

Lumension Endpoint Management and Security Suite (Lumension EMSS) is an Internet application that conforms to standard Web conventions. You can access the application's console from a Web browser. Log in to the Lumension EMSS Server to begin using product features.

**Prerequisites:**

Microsoft Internet Explorer 7, Microsoft Internet Explorer 8, or Mozilla Firefox 3.5.x. must be installed.

You can access the console from any endpoint within your network.

1. Open your Web browser.
2. In your browser’s address bar, type the Lumension EMSS URL (http[s]://*ServerIPAddress*).

3. Press ENTER.

   **Step Result:** The ***Connect to*** dialog opens.

The server 10.10.10.10 at 10.10.10.10 requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
TechPubsUser
Password:
Remember my password
OK
Cancel

Figure 1: Connect to Dialog

**Note:** If using Mozilla Firefox, the dialog appears differently.

4. Type your user name in the **User name** field.

   When logging in for the first time, type the user name of the Windows user account used to install Lumension EMSS. You can use additional user names after adding new user profiles to Lumension EMSS. If logging in using a domain account, type the name in the following format: `DOMAIN\Username`.

5. Type your password in the **Password** field.
6. Click **OK**.

**Result:** Lumension EMSS opens to the ***Home*** page.

## Logging Out of Lumension Endpoint Management and Security Suite

After you finish using Lumension Endpoint Management and Security Suite (Lumension EMSS), log out of the system to ensure no unauthorized users access the console.

1. Browse to the navigation menu.

2. Click **Log Out**.

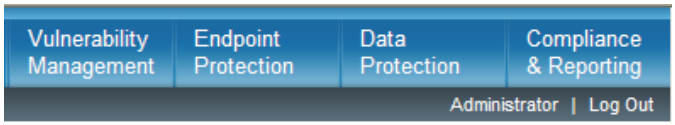



Figure 2: Log Out Link

**Result:** You are logged out of Lumension EMSS, and the ***Logout*** page displays.

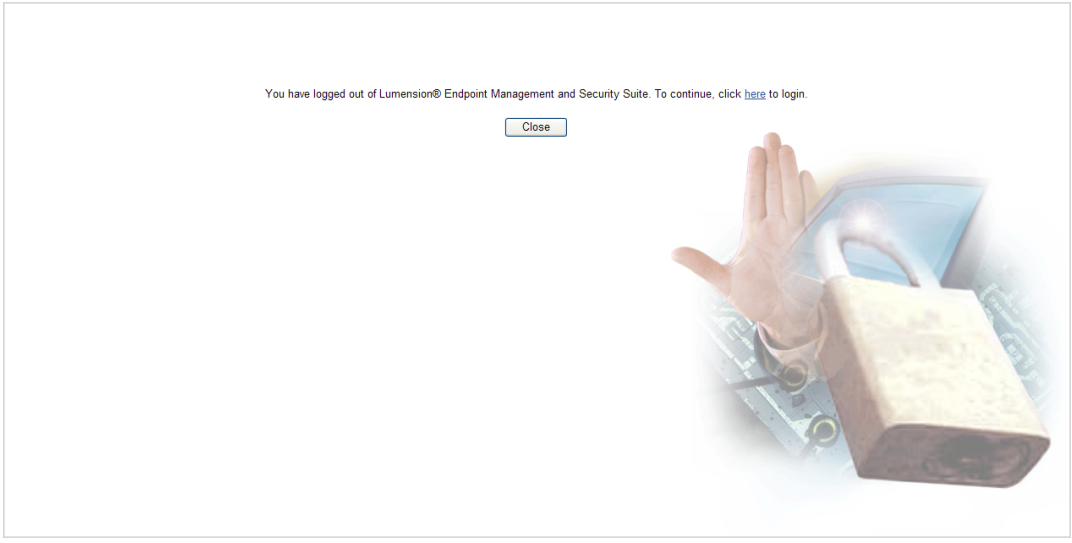



Figure 3: Log Out Page

## Common Functions within Lumension Endpoint Management and Security Suite

Lumension Endpoint Management and Security Suite (Lumension EMSS) uses both standard Web browser conventions and functions specific to itself. Familiarity with these common functions facilitate efficient product use.

From the navigation menu and system pages, you can access all features and functions your access rights authorize. The topics that follow provide instructions on how to use common functions.

## Common Conventions

This application supports user interface conventions common to most Web applications.

Table 5: Common User Interface Conventions

| Screen Feature | Function |
|---|---|
| **Entry Fields** | Type data into these fields, which allow the system to retrieve matching criteria or to enter new information. |
| **Drop-Down Menus** | Displays a list to select preconfigured values. |
| **Command Buttons** | Perform specific actions when clicked. |
| **Check Boxes** | A check box is selected or cleared to enable a feature, disable a feature, or initiate function for a list item. Some lists also include a **Select All** check box that lets you select all the available listed items on that page. |
| **Radio Buttons** | Select the button to select an item. |
| **Sort** | Data presented in tables can be sorted by ascending (default) or descending order within a respective column by clicking on a (enabled) column header. |
| **Mouseovers** | Additional information may be displayed by hovering your mouse pointer over an item. |
| **Auto Refresh** | Where present and when selected, the auto refresh function automatically refreshes the page every 15 seconds. |
| **Scrollbars** | Drag to see additional data that does not fit the window. |
| **Tabs** | Click on the tab name to switch to different information related to the specific page or dialog. |
| **Bread Crumb** | Names the page you are currently viewing, that page's parent page (if applicable), and the navigation menu item that opened the displayed page. If viewing a page that is child of another page, you can view the parent page by clicking the bread crumb, which also serves as a link, allowing you to retrace your steps. |
| **Tip:** Most system pages support right-click. | |

## Toolbars

**Toolbars** appear near the top of most system pages. These toolbars contain menus and buttons that let you use product features specific to the displayed page.

The menus and buttons displayed vary according to page. Additionally, user access rights determine which buttons are available for use. Click the available buttons and menus to use them.

Figure 4: Toolbar

## List Pages

Most Lumension Endpoint Management and Security Suite pages feature lists of selectable items. These items represent a series of product features that can be edited using menus and buttons.

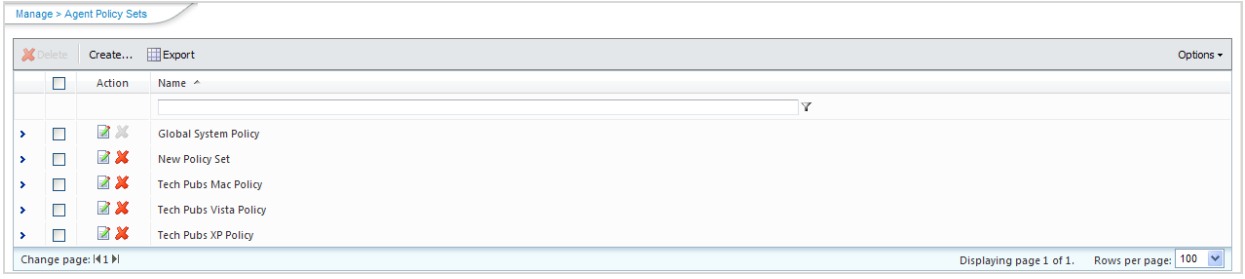



Figure 5: List Page

You can select individual list items. To select a list item:

- Select a check box.
- Click a list row.

You can select multiple list items. To select multiple list items:

- Select all list items by selecting the **Select All** check box.
- Select multiple, non-concurrent items by using `CTRL+Click` over list rows or check boxes.
- Select multiple, concurrent items by using `SHIFT+Click` over list rows or check boxes.

## The Options Menu

Toolbars feature an **Options** menu, whose function is to set page views, filter data, and enable clipboard copy. Menu items vary based on the functions applicable to the selected page.

The following functions can be found on the **Options** menu.

Table 6: Options Menu Items

| Option | Description |
|---|---|
| **Show results on page load** | If enabled, automatically provides query results based on the default filters. If disabled, you must define the available page filters and click **Update View** to view query results. For more information, see *Filters* on page 32. |

| Option | Description |
|---|---|
| **Save as default view** | Saves the current visual setting as the default view for the selected page and the logged in user. |
| **Clear default view** | Resets a saved default view to the system default view.<br>**Note:** This option is only available on certain pages. |
| **Show Group By Row** | Sorts list items into groups based on column headers. For more information, see *Group By* on page 35. |
| **Enable Copy to Clipboard** | Enables selected text to be copied to the clipboard and pasted into a text editor.<br>**Note:** Selecting this option disables other features, such as the right-click context menu, or dragging to select multiple list items. |
| **Note:** Some menu item titles change according to context. For example, if you select **Show Group By Row** to view the **Group By** row, the menu item title changes to **Hide Group By Row**. | |

## Filters

**Filters** appear on most list pages. You can use them to search pages for specific data.

Depending on which page you viewing, you can filter pages using one of the following features. Only one feature appears per page.

- Filters
- Filter Row

### Filters

Filters appear above page lists. They feature different fields, lists, and check boxes used for filtering. Filters vary according to page.

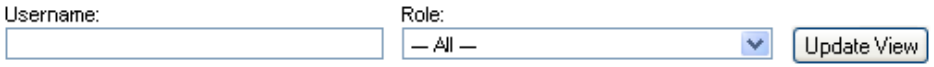



Figure 6: Filters

Additionally, you can save frequently used filter settings as your default view. To save your filter criteria, select a list page and choose **Options** > **Save as default view** from the toolbar. The toolbar **Options** menu contains the following options related to filtering.

Table 7: Filter Options

| Option | Function |
|---|---|
| **Show results on page load** | Automatically retrieves and displays results when selected. |

| Option | Function |
|---|---|
| **Save as default view** | Saves the active filter and sort criteria as the default view for the page.<br>The default view displays each time the page is accessed. You can change this setting at any time. |
| **Clear default view** | Resets a saved default view to the system default view. |

**Note:** Your default view remains applicable until you save a new default view or clear the default view, even after browsing to a different page or logging out of Lumension Endpoint Management and Security Suite.

### Filter Rows

Filter rows appear in the lists themselves. Rows feature a field for each column. Columns can be filtered using a variety of data types. For example, you can use a **Contains** filter or a **StartsWith** filter.

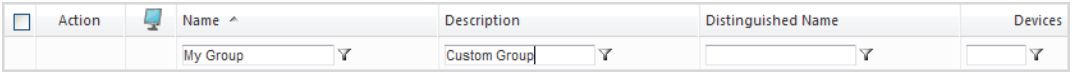



Figure 7: Filter Row

These filter are not case sensitive. Additionally, date columns filter at the lowest level of granularity; higher levels of granularity return no filter results.

## Using Filters

Use filters to search for specific list items when performing other tasks.

Filters are available on most list pages.

1. Select a list page. For additional information, refer to *List Pages* on page 31.
2. Ensure filters are displayed.
   If filters are not displayed, click **Show Filters**.
3. Define filter criteria.

   **Note:** Available filters differ by page.

   - In filter fields, type the desired criteria.
   - From filter lists, select the desired list item.
4. If applicable, select the **Include sub-groups** check box.

   **Note:** This check box only appears on list pages related to groups.
5. Click **Update View**.

   **Step Result:** The list is filtered according to the filter criteria.
6. If desired, save the filter criteria by selecting **Options** > **Save as default view** from the toolbar.

## Using Filter Rows

Some list pages use filter rows rather than filters. Use these rows, which are the first row of applicable lists, to filter column results.

These rows appear on several list pages.

1. Select a page featuring the filter row.
2. Ensure the filter row is displayed.
   If the filter row is not displayed, select **Options** > **Show Filter Row** from the toolbar.
3. Type criteria in the applicable filter row field.
4. Apply a filter type.
   a) Click the applicable **Filter** icon.

      **Step Result:** A menu opens.

   b) Select a filter type.
      The following table describes each filter type.

Table 8: Data Filtering Types

| Type | Description |
|---|---|
| **NoFilter** | Removes previously applied filtering. |
| **Contains** | Returns results that contain the value applied to the filter. |
| **DoesNotContain** | Returns results that do not contain the value applied to the filter. |
| **StartsWith** | Returns results that start with the value applied to the filter. |
| **EndsWith** | Returns results that end with the value applied to the filter |
| **EqualTo** | Returns results equal to the value applied to the filter. |
| **NotEqualTo** | Returns results that are not equal to the value applied to the filter. |
| **Greater Than** | Returns results that are greater than the value applied to the filter. |
| **Less Than** | Returns results that are less than the value applied to the filter. |
| **GreaterThanOrEqualTo** | Returns results that are greater than or equal to the value applied to the filter. |
| **LessThanOrEqualTo** | Returns results that are less than or equal to the value applied to the filter. |
| **Between** | Returns results that are between two values. Place a space between the two values. |
| **NotBetween** | Returns results that are not between two values. Place a space between the values. |
| **IsEmpty** | Returns results that are empty. |

| Type | Description |
|---|---|
| **NotIsEmpty** | Returns results that are not empty. |
| **IsNull** | Returns results that have no value. |
| **NotIsNull** | Returns results that have a value. |

**Note:** Text filters are case sensitive. Date columns filter at the lowest level of granularity; higher levels of granularity return no filter results. The availability of filtering options is dependent on the type of data displayed in the column. For example, filtering options that can only apply to numeric data will not be available in columns that contain text data or a mix of text and numeric data.

**Result:** The list column is filtered according to the criteria. If desired, repeat the process to filter additional columns.

## Group By

The **Group By** row lets you sort list items into groups based on column headers.

To use the **Group By** row, ensure **Options** > **Show Group By Row** is selected from the toolbar, and then drag a column header into the row. You may drag multiple columns to the row, but you may only drag one column into the row at a time.

To ungroup the list, right-click on the row and select **Cancel All Groupings**. To hide the **Group By** row, select **Options** > **Hide Group By Row**.

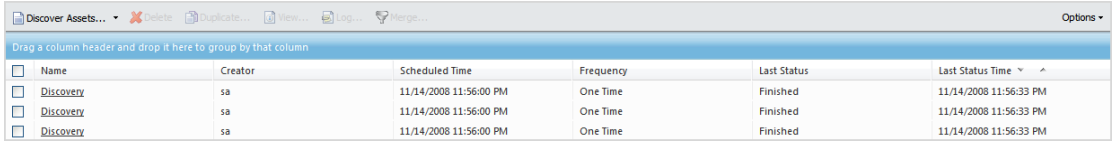



Figure 8: Group By Row

## Expanding and Collapsing Structures

Certain structures in Lumension Endpoint Management and Security Suite are expandable and collapsible. Expand structures to view additional available information or options. Collapse them to conserve screen space.

Click available **Plus** icons (+), **Minus** icons (-), and **Rotating Chevron** icons (>) to expand or collapse a structure.

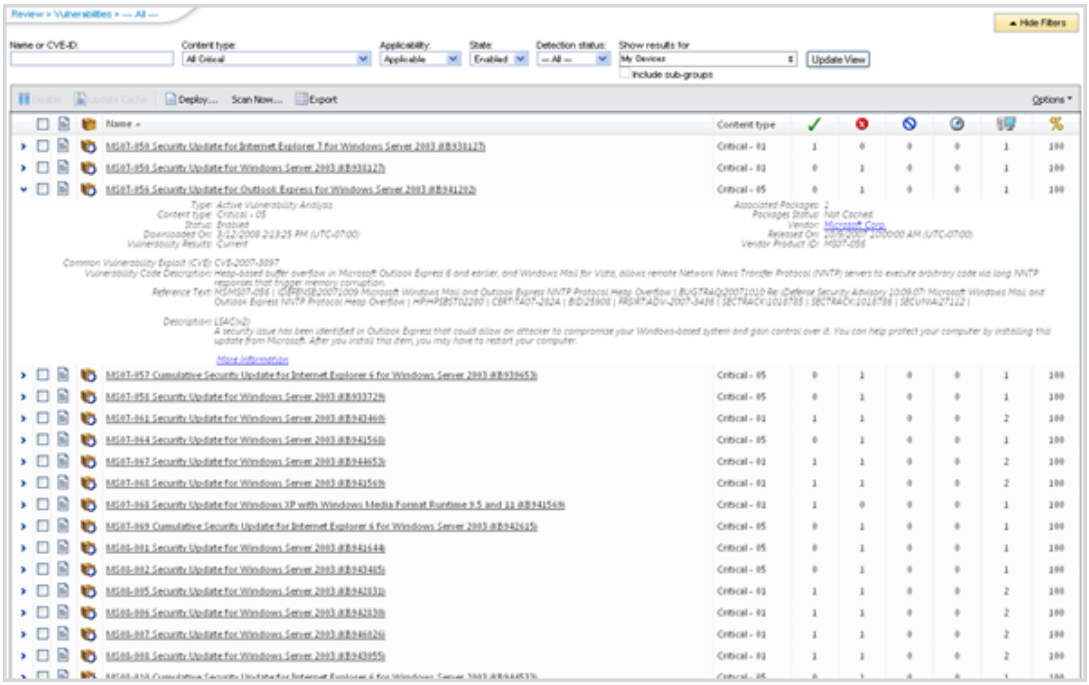


Figure 9: Expandable/Collapsable Structure Example

## Advancing Through Pages

Lumension Endpoint Management and Security Suite features links to page through large lists.

Click the links to page through lists. The number of list items and the specific page you are viewing determines the number of pagination links.

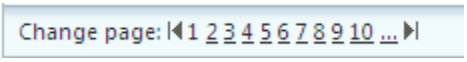



Figure 10: Pagination Feature

Lumension Endpoint Management and Security Suite also features a **Rows Per Page** drop-down list. From this list, you can select the number of items that populate a list.

Table 9: Pagination Feature Functions

| Icon or Link | Title | Function |
|---|---|---|
| ▶\| | **Final Page Link** | Advances to the final page of list items. |
| \|◀ | **First Page Link** | Returns to the first page of list items. |
| ... | **Next Ten/Previous Ten Pages Link** | Displays the next ten or previous ten page links available. Fewer page links will display if the remaining list items cannot populate ten pages. |
| 4 5 6 | **Pagination Links** | Advances or returns to the selected pagination link. |

Each page also features a **Rows Per Page Drop-Down List**. This list modifies the number of list items displayed on a single page (25, 50, 100, 200, 500).

## Help

Lumension Endpoint Management and Security Suite contains context-sensitive HTML (`.html`) help. Help provides product feature explanations, step-by-step procedures, and reference materials.

Accessing help differs according to context.

- From a page, select **Help** > **Help Topics**.
- From a dialog, click the **Question Mark** icon (**?**).

Accessing help displays information that is useful for your current context.

## Exporting Data

On many system pages, you can export the listed data to a comma separated value file (`.csv`) available for use outside of Lumension Endpoint Management and Security Suite (Lumension EMSS). Use this exported data for management purposes (reporting, noting trends, and so on).

You can export data from a variety of Lumension EMSS pages.

**Note:** These instructions are intended for Microsoft Internet Explorer users. If you are using Mozilla Firefox, this procedure differs slightly.

**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

1. Select a list page (or dialog) where you can export information.
2. If necessary, populate the page by defining filter criteria and clicking **Update View**.
3. Click **Export**.

   **Step Result:** The ***File Download*** dialog opens.

4. In the ***File Download*** dialog, select from one of the following options.

| Option | Description |
|---|---|
| **Open** | Creates the file and opens it in your default (`.csv`) program. |
| **Save** | Creates the file and saves it to a specified local folder. The file is saved in a Microsoft Office Excel (`.csv`) format. The file is named *`Export.csv`*, with the exported file containing data based on list data. |
| **Cancel** | Cancels the export. |

**Note:** All data results will export, not just the selected results.

| | A | B | C |
|---|---|---|---|
| 1 | Device Name | Hardware Class | Hardware Item |
| 2 | \\TP-VAGENT | Architecture | x86 |
| 3 | \\TP-VAGENT | Batteries | Microsoft AC Adapter |
| 4 | \\TP-VAGENT | BIOS | PTLTD - 6040000 PhoenixBIOS 4.0 Release 6.0 Date: 07/22/08 |
| 5 | \\TP-VAGENT | BIOS Asset Tag | No Asset Tag |
| 6 | \\TP-VAGENT | Computer | ACPI x86-based PC |
| 7 | \\TP-VAGENT | Computer | OS Serial Number = 55041-037-8318942-71732 |
| 8 | \\TP-VAGENT | Computer | Virtualization = VMWare |
| 9 | \\TP-VAGENT | Disk drives | VMware Virtual disk SCSI Disk Device |
| 10 | \\TP-VAGENT | Display adapters | VMware SVGA II |
| 11 | \\TP-VAGENT | DVD/CD-ROM drives | NECVMWar VMware IDE CDR00 ATA Device |
| 12 | \\TP-VAGENT | File Systems | C:\ Type:NTFS Free:0.961 GB Total:7.997 GB |
| 13 | \\TP-VAGENT | Floppy disk drives | Floppy disk drive |
| 14 | \\TP-VAGENT | Floppy drive controllers | Standard floppy disk controller |
| 15 | \\TP-VAGENT | IDE ATA/ATAPI controllers | ATA Channel 0 |
| 16 | \\TP-VAGENT | IDE ATA/ATAPI controllers | Intel(R) 82371AB/EB PCI Bus Master IDE Controller |

Figure 11: Exported Data

# The Home Page

The entry point to Lumension Endpoint Management and Security Suite (Lumension EMSS) is the ***Home*** page. From this page you can view the dashboard, which features draggable widgets that display information about Lumension EMSS and agent-managed endpoints.

Some widgets display general information about the system, others provide links to documentation, and still others summarize activity for Lumension EMSS modules you are licensed for.

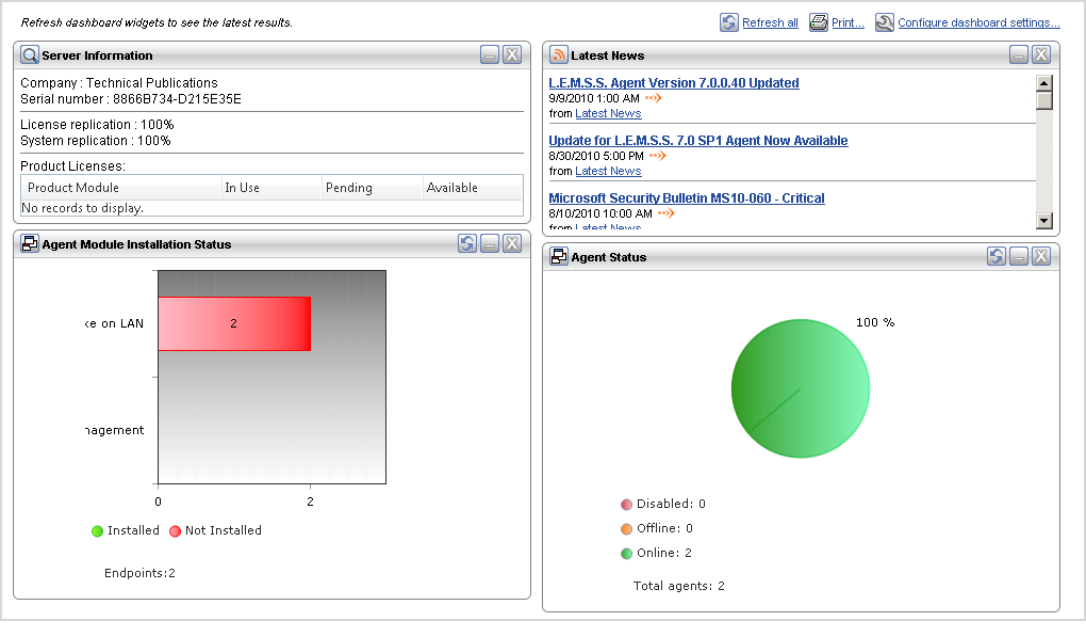



Figure 12: The Home Page

## The Lumension Endpoint Management and Security Suite Header

The product header appears at the top of all Lumension Endpoint Management and Security Suite Web site pages.

Figure 13: Header

This header contains links for information about various Lumension products. Clicking one of these links opens a new window that pertains to the applicable product.

## The Navigation Menu

This menu appears on all Lumension Endpoint Management and Security Suite pages. Use this menu to navigate through the console.

This menu organizes product features based on functionality. When you select a menu item (or sub-menu item), a new page, dialog, wizard, or window opens. You can access all features of the system from this menu (that your access rights authorize).

**Note:** The menu items available change based on the installed Lumension Endpoint Management and Security Suite modules.

Figure 14: Navigation Menu

The navigation menu contains the several menus, which are organized based on functionality.

Table 10: Navigation Menus

| Menu | Description |
|---|---|
| **Home** | Opens the ***Home*** page. This link contains no menu items. |
| **Discover** | Contains menu items related to running discovery scan jobs. |
| **Review** | Contains menu items related to reviewing security content and discovery scan jobs. |
| **Manage** | Contains menu items related to managing system features. |
| **Reports** | Contains menu items related to creating reports. |
| **Tools** | Contains menu items related to system administration. |
| **Help** | Contains menu items related to help systems. |

**Tip:** When a menu item is selected, the navigation menu text is underlined to display its active state.

Most navigation menus contain items. The following table lists each menu item in the **Discover** menu and the actions that occur when they are selected.

Table 11: Discover Menu Items

| Menu Item | Description |
|---|---|
| **Assets...** | The ***Discover Assets*** dialog. |
| **Assets and Install Agents...** | The ***Install Agents*** dialog. |
| **Assets and Uninstall Agents...** | The ***Uninstall Agents*** dialog. |

The following table lists each menu item in the **Review** menu and the actions that occur when they are selected.

Table 12: Review Menu Items

| Menu Item | Description |
|---|---|
| **Asset Discovery Job Results** | Opens the ***Job Results*** page, which is filtered to display discovery job results. |
| **Agent Management Job Results** | Opens the ***Job Results*** page, which is filtered to display agent management job results. |

The following table lists each menu item in the **Manage** menu and the actions that occur when they are selected.

Table 13: Manage Menu Items

| Menu Item | Description |
|---|---|
| **Endpoints** | Opens the ***Endpoints*** page. |
| **Groups** | Opens the ***Groups*** page. |
| **Agent Policy Sets** | Opens the ***Agent Policy Sets*** page. |

The following table lists each menu item in the **Reports** menu and the actions that occur when they are selected.

Table 14: Reports Menu Items

| Menu Item | Description |
|---|---|
| **All Reports** | Opens the ***All Reports*** page. |
| **Configuration** | Opens the ***All Reports*** page with configuration reports expanded. |
| **Inventory** | Opens the ***All Reports*** page with inventory reports expanded. |
| **Policy and Compliance** | Opens the ***All Reports*** page with policy and compliance reports expanded. |

The following table lists each menu item in the **Tools** menu and the actions that occur when they are selected.

Table 15: Tools Menu Items

| Menu Item | Description |
|---|---|
| **Users and Roles** | Opens the ***Users and Roles*** page. |
| **Change My Password...** | Opens the ***Change My Password*** dialog. |
| **Download Agent Installer...** | Opens the ***Download Agent Installer*** dialog opens over the currently selected page. |
| **Launch Installation Manager...** | Opens the ***Lumension Installation Manager*** in a new window. |
| **Subscription Updates** | Opens the ***Subscription Updates*** page. |

| Menu Item | Description |
|---|---|
| **Directory Sync Schedule** | Opens the ***Directory Sync Schedule*** page. |
| **Email Notifications** | Opens the ***Email Notifications*** page. |
| **Options** | Opens the ***Options*** page. |

The following table lists each menu item in the **Help** menu and the actions that occur when they are selected.

Table 16: Help Menu Items

| Menu Item | Description |
|---|---|
| **Help Topics...** | Opens the ***Help*** page. |
| **Help Forums...** | Opens the Lumension message boards. |
| **Knowledge Base...** | Opens the Lumension knowledge base. |
| **New Users Start Here...** | Opens the ***New Users Start Here*** page. |
| **Technical Support** | Opens the ***Technical Support*** page. |
| **Product Licensing** | Opens the ***Product Licensing*** page. |
| **About...** | Opens the ***About*** dialog. |

**Note:** Any unavailable or absent menus, menu items, or sub-menu items are due to restricted access rights or unavailable modules. Contact your network administrator if you require access to unavailable features.

## The Dashboard

The **dashboard** displays widgets depicting the activity on your protected network. Located on the ***Home*** page, the dashboard provides convenient information you can use to ensure your network protection is up to standard. Additionally, you can customize the dashboard to display the widgets most applicable to your network environment.

Widget graphs are generated based on the latest data and statistics available from endpoints, groups, module-specific data, and so on.

The following ***Dashboard*** widgets are available:


- *The Agent Module Installation Status Widget* on page 43
- *The Agent Status Widget* on page 44
- *The Discovery Scan Results: Agent Widget* on page 45
- *The Last Five Completed Scan Jobs Widget* on page 46
- *The Latest News Widget* on page 46
- *The Next Five Pending Scan Jobs Widget* on page 47
- *The Server Information Widget* on page 47

## The Agent Module Installation Status Widget

This widget displays the installation and licensing stats of each agent module.

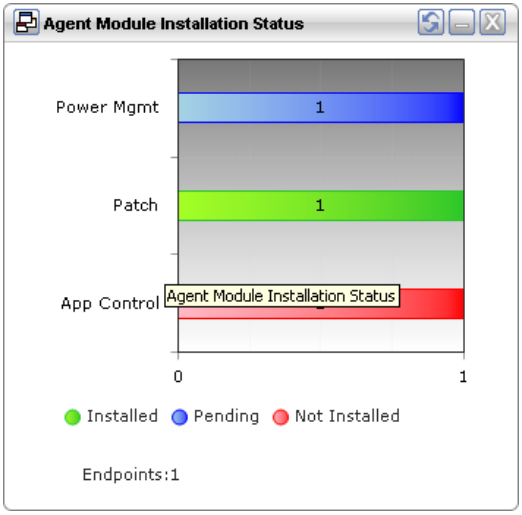



Figure 15: Agent Module Installation Status Widget

A graph bar displays for each installed module. The following table describes the widget graph(s).

Table 17: Graph Bar Color Descriptions

| Bar Color | Description |
|---|---|
| **Blue** | The number of managed endpoints with the applicable module pending installation or uninstallation. |
| **Green** | The number of managed endpoints with the applicable module installed. |
| **Red** | The number of managed endpoints without the applicable module installed. |

**Tip:** Click the graph to open the ***Endpoints*** page ***All*** tab.

**Note:** Endpoints with an agent version that does not support a module are not counted.

### The Agent Status Widget

This widget displays all agents grouped by agent status.

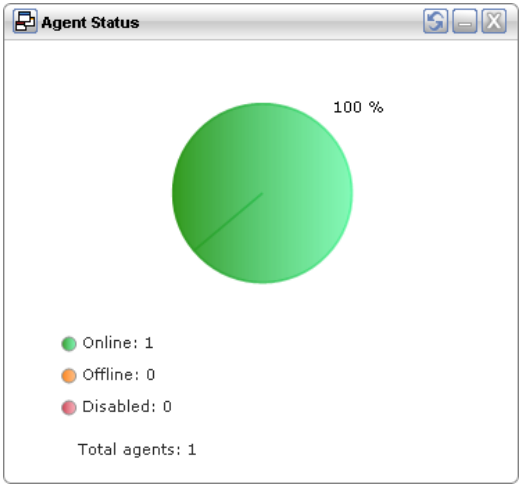



Figure 16: The Agent Status Widget

The following table describes the fields in the **Agent Status** widget.

Table 18: Agent Status Widget Fields

| Field | Description |
|---|---|
| **Online** | The number of agents that are online. |
| **Offline** | The number of agents that are offline.<br>**Note:** Offline status is determined by the amount of time since the agent last communicated as determined on the ***Options*** page. |
| **Disabled** | The number of agents that are disabled. |
| **Total Agents** | The total number of agents in your environment. |
| **Tip:** Clicking on the pie chart opens the ***Endpoints*** page ***All*** tab. The page is filtered to display all agents. | |

## The Discovery Scan Results: Agent Widget

This widget displays the number endpoints capable of hosting agents (agent-compatible endpoint) discovered in the latest discovery scan job. The endpoints discovered are classified in to two groups: endpoints with agents and endpoints without agents.

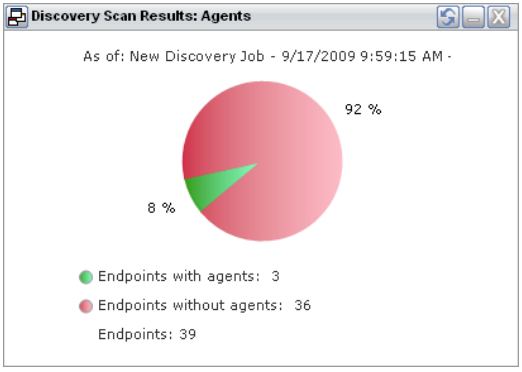

Discovery Scan Results: Agents
As of: New Discovery Job - 9/17/2009 9:59:15 AM -
92 %
8 %
Endpoints with agents: 3
Endpoints without agents: 36
Endpoints: 39

Figure 17: Discovery Scan Results Widget

The following table describes the **Discovery Scan Results: Agent** widget fields.

Table 19: Discovery Scan Results Widget Fields

| Field | Description |
|---|---|
| **As of** | The name of the discovery scan job used to generate the widget graph and statistics. This job is the job most recently run. |
| **Endpoints with agents** | The number of agent-compatible endpoints discovered that have agents installed. |
| **Endpoints without agents** | The number of agent-compatible endpoints discovered that have no agents installed. |
| **Endpoints** | The total number of agent-compatible endpoints discovered. |

**Tip:** Clicking the **Discovery Scan Results: Agent** widget opens the ***Results*** page for the most recently run discovery scan job.

### The Last Five Completed Scan Jobs Widget

This widget contains information about the last five completed scan jobs. Each job name is a link to the associated ***Result*** page.

Figure 18: Last Five Completed Scan Jobs Widget

The following table describes each column in the **Last Five Completed Jobs** widget.

Table 20: Last Five Completed Scan Jobs Widget Columns

| Column | Description |
|---|---|
| **Name** | The job name. The name is a link to the associated ***Results*** page. |
| **Completed Date** | The date and time the job completed on the server. |
| **Status** | The status of the completed job. |

### The Latest News Widget

This widget displays important announcements and other information regarding Lumension Endpoint Management and Security Suite.

Click a ***Latest News*** link to view additional details about an announcement in a new window.

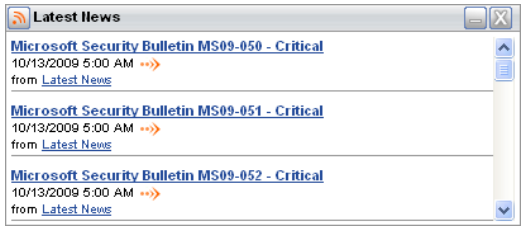



Figure 19: Latest News Widget

## The Next Five Pending Scan Jobs Widget

This widget displays information about the next five pending discovery scan jobs. Each job name is a link to the ***Discovery Scan Jobs*** page ***Scheduled*** tab.

Figure 20: Next Five Pending Scan Jobs Widget

The following table describes the **Next Five Pending Scan Jobs** widget columns.

Table 21: Next Five Pending Scan Jobs Widget Columns

| Column | Description |
|---|---|
| **Name** | The job name. Each name is a link to the ***Discovery Scan Jobs*** page ***Scheduled*** tab. |
| **Scheduled Time** | The date and time the job is scheduled to run on the server. |

## The Server Information Widget

This widget lists your serial number, number of licenses available, number of licenses in use, and information about current license usage and availability for Lumension Endpoint Management and Security Suite (Lumension EMSS).

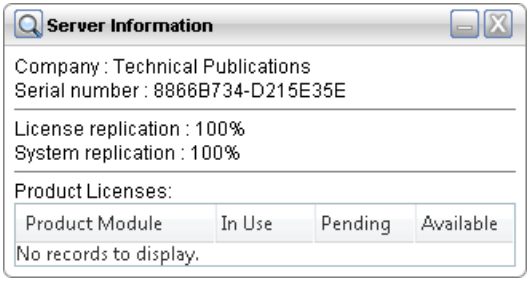



Figure 21: Server Information Widget

The following table describes the fields in the **Server Information** widget.

Table 22: Server Information Widget Fields

| Field Name | Description |
|---|---|
| **Company** | The company Lumension EMSS is registered to as defined during installation. |
| **Serial number** | Lumension EMSS license number (serial number) assigned to your server. |

| Field Name | Description |
|---|---|
| **License replication** | The subscription status between Lumension EMSS and the Global Subscription Server (GSS). |
| **System replication** | The system replication status between Lumension EMSS and the GSS. |

The following table describes the **Product Licenses** table columns. A row appears for each purchased module.

Table 23: Product Licenses Table Columns

| Column | Description |
|---|---|
| **Product Module** | The module for which you purchased licenses. |
| **In Use** | The number of module licenses in use. |
| **Pending** | The number of licenses pending use or pending removal. Licenses pending removal become available upon removal completion. |
| **Available** | The number of licenses available. |

**Note:** A license expiration notice displays if all available licenses are expired.

## Dashboard Setting and Behavior Icons

Setting and behavior icons are UI controls used to manage the dashboard. Click these icons to maximize, minimize, hide, and refresh the dashboard and widgets.

The following table describes each icon action.

Table 24: Widget Setting and Behavior Icons

| Icon | Action |
|---|---|
| | Opens the ***Dashboard Settings*** dialog. |
| | Opens the dashboard in print preview mode. |
| | Collapses the associated widget. |
| | Expands the associated collapsed widget. |
| | Hides the associated widget. |
| | Refreshes the associated widget (or the entire dashboard). |

**Note:** Not all widgets contain **Refresh** icons.

## Previewing and Printing the Dashboard

When viewing the dashboard, you can reformat it for printing purposes. This print preview omits the Web site's header and footer, reorganizing the dashboard to display only the selected widgets, making it ideal for printing.

View the print preview from the ***Home*** page.

1. Select **Home** from the navigation menu.
2. Click the **Print** icon.

   **Step Result:** The dashboard print preview opens in a new Web browser window.

3. If desired, use your Web browser controls to print the dashboard.

## Editing the Dashboard

Lumension Endpoint Management and Security Suite lets you define how dashboard widgets are arranged and prioritized. Edit the dashboard to display only the widgets that are most useful when managing your network environment.

Edit the dashboard from the ***Dashboard Settings*** dialog.

1. From the navigation menu, select **Home**.
2. Click the **Settings** icon.

   **Step Result:** The ***Dashboard Settings*** dialog opens.

Dashboard Settings
Agent Status
This chart displays all agents grouped by status.
Discovery Scan Results
This chart displays the total number of endpoints discovered in the last-run Discovery Scan job and identifies how many had an agent installed.
Endpoint Patch Status
This chart displays all endpoints with applicable critical vulnerabilities grouped by age and the patch status within each category.
Incomplete Deployments
This chart displays all deployments whose start dates have elapsed that have a status of 'not started' or 'in progress'.
Last 5 Completed Scan Jobs
This chart displays a list of the last 5 completed jobs and their status.
Latest News
This displays a feed of the latest security bulletins and product information.
Mandatory Baseline Compliance
Descriptions:
Columns:
OK
Cancel

Figure 22: Dashboard Settings Dialog

3. Choose which widgets you want to display on the dashboard.
   - Select the check box associated with the applicable widget to display it.
   - Clear the check box associated with the applicable widget to hide it.
4. Prioritize the widgets in the desired order.

- Click the applicable **Increase Priority** icon to increase a widget priority.
- Click the applicable **Decrease Priority** icon to decrease a widget priority.

Highly prioritized widgets appear in the dashboard upper-left corner, while lowly prioritized widgets appear in the lower-right.

5. Display or hide widget descriptions.

   - Click the **Display Descriptions** icon to display descriptions.
   - Click the **Hide Descriptions** icon to hide description.

6. Choose a widget layout.

   - Click the **Two Column** icon to make widgets appear in two columns.
   - Click the **Three Column** icon to make widgets appear in three columns.

7. Click **OK**.

## The System Alert Pane

The ***System Alert*** pane is an expandable window that provides information about changing conditions on your Lumension Endpoint Management and Security Suite server. The System Alert pane displays information about required actions with links to related help topics to assist you with tasks.

The System Alert pane displays on the left side of the dashboard and shows the number of alerts that require your attention. You can drag the right edge of the pane to resize the System Alert pane within the dashboard.

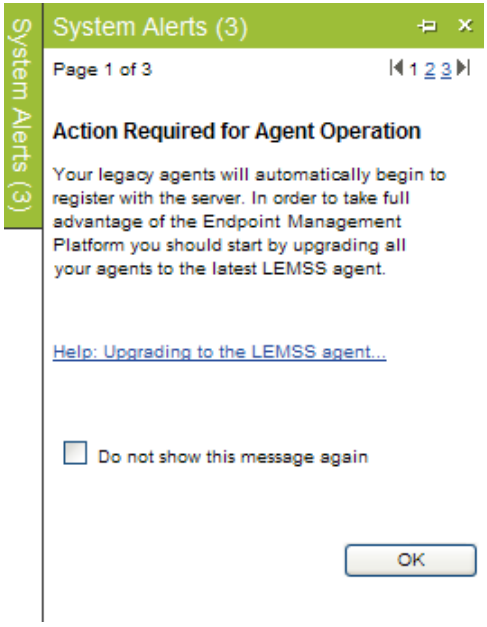

System Alerts (3)
System Alerts (3)
Page 1 of 3
1 2 3
Action Required for Agent Operation
Your legacy agents will automatically begin to register with the server. In order to take full advantage of the Endpoint Management Platform you should start by upgrading all your agents to the latest LEMSS agent.
Help: Upgrading to the LEMSS agent...
Do not show this message again
OK

Figure 23: The System Alert Pane

The following functions can be found in the ***System Alert*** pane.

Table 25: Options Menu Items

| Option | Description |
|---|---|
| **Pin** (icon) | Docks the System Alert pane open. Clicking this icon again will collapse the System Alert pane. |
| **Pagination Links** | Allows you to navigate between alerts. For more information, see *Advancing Through Pages* on page 36. |
| **Action Link** | Opens the appropriate application page, external Web page, or context-sensitive help topic, depending on the action specified in the alert. |
| **Don't show this again** (check box) | Collapses the ***System Alert*** pane. The alert shown in the ***System Alert*** pane when this check box is selected will no longer be shown. |
| **OK** (button) | Collapses the ***System Alert*** pane. |

**Note:** Dismissing a notification only dismisses the notification for the user you are currently logged in as. The notification still displays for other users. Additionally, the system automatically dismisses alerts as you complete their related actions, regardless of whether you manually dismiss those alert.

## License Expiration

The Lumension Endpoint Management and Security Suite and its modules are licensed for a prepaid period. When you purchase a module, you purchase a license for the module itself and the module function for a set number of agents. After the license period expires, you must renew your licenses.

The following table describes the different licensing expiration scenarios and the events that follow.

**Note:** When a subscription expires, the applicable module history and configuration is retained so no work is lost when the module is renewed.

Table 26: License Expiration Scenario and Events

| Scenario | Event(s) |
|---|---|
| Lumension EMSS Module Expiration | • All menu items and features related to the module are disabled.<br>• Functionality for all agent components for the module is partially disabled (function disabled varies by module).<br>• Agent components for the module cannot be installed on agents that do not already have the module installed.<br>• *`Module`* `Installed` statuses for affected endpoints change from `Installed` to `Expired` on the ***Endpoints*** page.<br>• The **Available** license count for the module changes to `0` in the **Server Information** widget. |
| Lumension EMSS Module Agent Expiration | • Functionality for all agent components for the module (in the license block) is partially disabled (functions disabled varies by module).<br>• Agent components for the module cannot be installed on agents that do not already have the module installed.<br>• *`Module`* `Installed` statuses for affected endpoints change from `Installed` to `Expired` on the ***Endpoints*** page.<br>• The **Available** license count for the module changes to `0` in the **Server Information** widget. |

**Tip:** You can view subscription service history from *The Subscription Updates Page* on page 53. You can also view license information from *The Product Licensing Page* on page 91.

To reactivate your licenses following renewal, select the ***Subscription Updates*** page and click **Update Now**. The license verification process begins and connects to the Global Subscription Server, retrieving updated license information. The page refreshes following update completion, and all previous module functionality is restored.

**Note:** For more information about renewing or adding licenses, contact *Lumension Sales Support* (*patchlink.sales@lumension.com*).

# Chapter 3

# Configuring Default Behavior

**In this chapter:**


- The Subscription Updates Page
- Working with Subscription Updates
- The Email Notifications Page
- Working with Email Notifications
- The Options Page
- Working with Options


Use configuration options to define default behavior and administer Lumension Endpoint Management and Security Suite. Configure and manage the product using a variety of system Web pages.

The pages used to configure default behavior include:


- *The Subscription Updates Page* on page 53
- *The Email Notifications Page* on page 62
- *The Options Page* on page 70


## The Subscription Updates Page

Periodically, the Lumension Endpoint Management and Security Suite (Lumension EMSS) server renews license and system information via contact with the Global Subscription Server (GSS). If additional modules are installed, subscription updates downloads additional, module-specific information. You can view or edit settings related to this process from the ***Subscription Updates Page***.

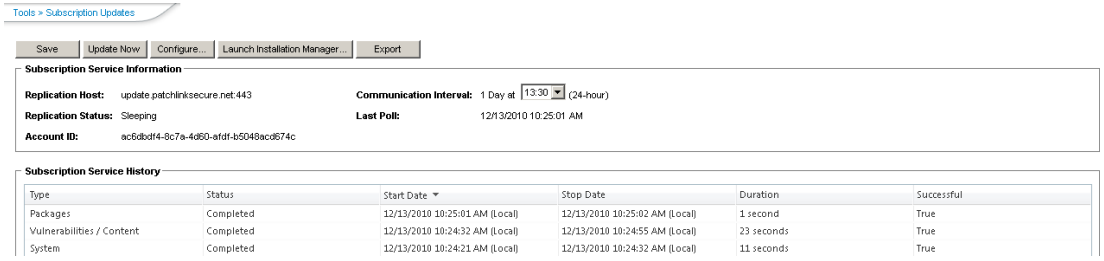

Tools > Subscription Updates
Save
Update Now
Configure...
Launch Installation Manager...
Export
Subscription Service Information
Replication Host: update.patchlinksecure.net:443
Communication Interval: 1 Day at 13:30 (24-hour)
Replication Status: Sleeping
Last Poll: 12/13/2010 10:25:01 AM
Account ID: ac6dbdf4-8c7a-4d80-afdf-b5048acd674c
Subscription Service History
Type | Status | Start Date | Stop Date | Duration | Successful
Packages | Completed | 12/13/2010 10:25:01 AM (Local) | 12/13/2010 10:25:02 AM (Local) | 1 second | True
Vulnerabilities / Content | Completed | 12/13/2010 10:24:32 AM (Local) | 12/13/2010 10:24:55 AM (Local) | 23 seconds | True
System | Completed | 12/13/2010 10:24:21 AM (Local) | 12/13/2010 10:24:32 AM (Local) | 11 seconds | True

Figure 24: Subscription Updates Page

From this page, you can modify the subscription communication interval, initiate a replication, and configure the subscription service. This page also displays the subscription service history, which lists previous replications. These listings confirm successful communication between the Lumension EMSS server and the GSS.

Subscription updates retrieve the latest data for the following Lumension EMSS items:

| | |
|---|---|
| **Licenses** | During communication with the GSS, Lumension EMSS verifies product license validity. |

| | |
|---|---|
| **System** | During communication with the GSS, Lumension EMSS downloads operating system definitions and agent updates. |

## Viewing the Subscription Updates Page

Navigate to the ***Subscriptions Updates*** page to view and edit subscription settings.

You can access this page from the navigation menu.

1. Select **Tools** > **Subscription Updates**.
2. Perform a task listed in *Working with Subscription Updates* on page 60.

## Subscription Updates Page Toolbar

This toolbar control the functions available from the ***Subscription Updates*** page.

Table 27: Subscription Updates Page Buttons

| Button | Function |
|---|---|
| **Save** | Saves the edits made to the subscription updates. You must click the button to implement your edits. |
| **Update Now** | Replicates all license, system, changes since the last replication with the Global Subscription Server (GSS). For additional information refer to *Replicating* on page 60. |
| **Configure...** | Configures subscription communication settings between the Lumension Endpoint Management and Security Suite server and the GSS. For additional information refer to *The Subscription Service Configuration Dialog* on page 56. |
| **Launch Installation Manager...** | Opens the Lumension Installation Manager in a new window. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |

## Subscription Service Information

These fields list information about the Global Subscription Server and its communication history with your Lumension Endpoint Management and Security Suite (Lumension EMSS) Server.

The following table describes the **Subscription Service Information** fields.

Table 28: Subscription Service Information

| Field | Description |
|---|---|
| **Replication Host** | The name and port of the Global Subscription Server (GSS). |
| **Replication Status** | The current replication status. Replication ensures that Lumension EMSS remains current with the latest license information. |
| **Account ID** | Your account ID. The ID is passed to the GSS, which validates the update request. The account ID is created by Lumension EMSS when it registers with the GSS. |
| **Communication Interval** (list) | The time Lumension EMSS connects to the GSS for replication. For additional information refer to *Editing the Communication Interval* on page 60. |
| **Last Poll** | The date and time of the last successful contact with the GSS. |

## Subscription Service History

This table lists a record of subscription license replications and content replications. Additional details for each replication is included.

The following reference describes the **Subscription Service History** table.

Table 29: Subscription Service History Table

| Column | Description | |
|---|---|---|
| **Type** | The type of replication task. The types include: | |
| | **`Licenses`** | Verifies the validity of your Lumension Endpoint Management and Security Suite licenses. |
| | **`System`** | Downloads new system files. |
| **Status** | The status of the replication task. The statuses include: | |
| | **`Initializing Replication`** | Replications are initializing. |
| | **`Downloading`** | Replications are downloading. |
| | **`Completed`** | Replications are complete. |
| **Start Date** | The date and time the task started. | |

| Column | Description |
|---|---|
| **Stop Date** | The date and time the task completed. |
| **Duration** | The duration of the task in minutes and seconds (*2 minute[s], 0 seconds*). |
| **Successful** | The replication task completion status (`True` or `False`). |

## The Subscription Service Configuration Dialog

This dialog is the interface used to configure subscription updates. Use this dialog to configure how your Lumension Endpoint Management and Security Suite (Lumension EMSS) server contacts the Global Subscription Server (GSS). Additionally, use this dialog to select the languages that content definitions are downloaded in.

The ***Subscription Service Configuration*** dialog contains the following tabs:

- *The Service Tab* on page 56

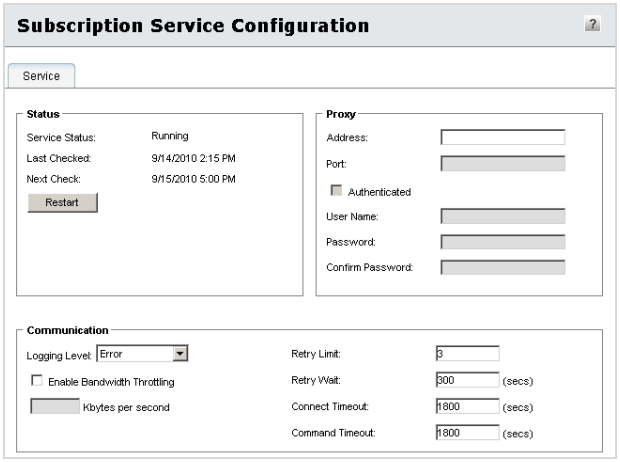



Figure 25: Subscription Service Configuration Dialog

### Viewing the Subscription Service Configuration Dialog

Navigate to this dialog to begin editing settings related to subscription services.

You can access this dialog from the ***Subscription Updates*** page.

1. Select **Tools** > **Subscription Updates**.
2. Click **Configure...**.

**Result:** The ***Subscription Service Configuration*** dialog opens.

### The Service Tab

Using this tab, you can customize communication settings between the Lumension Endpoint Management and Security Suite (Lumension EMSS) server and the Global Subscription Server, as well as the log recorded during transactions. Additionally, if your Lumension EMSS server uses a proxy server to access the Internet, you can

define your proxy server information using this tab. Finally, you can use this tab to restart the subscription service.

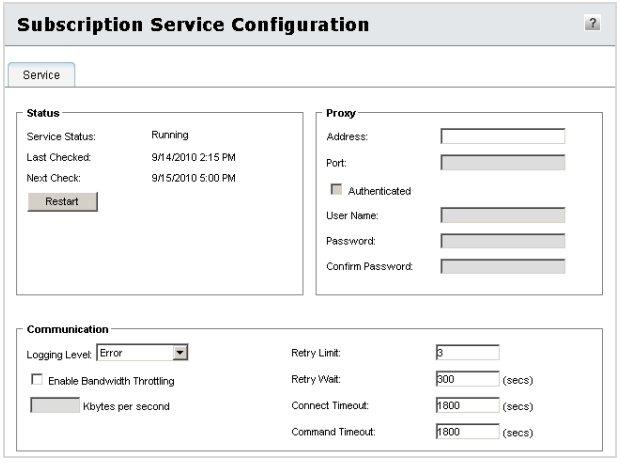



Figure 26: Service Tab

## Status

The **Status** section lists whether the subscription service is running, as well as information about past and pending communication with the Global Subscription Server (GSS). It also lets you restart the service. View this section for useful information when troubleshooting communication issues between the Lumension Endpoint Management and Security Suite server and the GSS.

The following table describes each **Status** field and control.

Table 30: Status Fields and Controls

| Field or Control | Description |
|---|---|
| **Service Status** (Field) | The current status of the local subscription service's communication with the GSS. |
| **Last Checked** (Field) | The last date and time the local subscription service contacted the GSS. |
| **Next Check** (Field) | The next scheduled date and time for the local subscription service to contact the GSS. |
| **Restart** (Button) | Restarts the subscription service. For additional information, refer to *Restarting the Subscription Service* on page 62. |

## Proxy

When using a proxy for communication between the Lumension Endpoint Management and Security Suite (Lumension EMSS) server and the Global Subscription Server (GSS), you must define the applicable proxy information within Lumension EMSS before communication can occur.

Define this proxy information from the ***Subscription Service Configuration*** dialog ***Service*** tab. The following table describes each setting.

Table 31: Proxy Setting Descriptions

| Setting | Description |
|---|---|
| **Address** (field) | The IP address or name of the proxy used for communication between Lumension EMSS and the GSS. |
| **Port** (field) | The proxy port used for communication between Lumension EMSS and the GSS. |
| **Authenticated** (check box) | This check box enables the remaining fields when proxy authentication is required. |
| **User Name** (field) | A user name that will authenticate with the proxy. |
| **Password** (field) | The password associated with the user name. |
| **Confirm Password** (field) | The password retyped. |

## Communication

When configuring subscription service communication, you can define multiple parameters regarding how your Lumension Endpoint Management and Security Suite server communicates with the Global Subscription Server.

Define communication options from the ***Subscription Service Configuration*** dialog ***Service*** tab. The following table describes each communication option.

Table 32: Communication Option Descriptions

| Option | Description |
|---|---|
| **Logging Level** (list) | Defines the level of detail in logs recorded during communication between the Lumension Endpoint Management and Security Suite server and the Global Subscription Server. The available values include:<br>**Debug** — Logs errors, warnings, system actions, and debugging information.<br>**Note:** This logging level is the most comprehensive logging level. It should only be used for troubleshooting purposes due to the large logging files it produces and increased replication overhead it causes.<br>**Information** — Logs errors, warnings, and system actions.<br>**Warning** — Logs errors and warnings.<br>**Error** — Logs only errors. |
| **Enable Bandwidth Throttling** (check box) | Limits the maximum data quantity during communication between the Lumension Endpoint Management and Security Suite server and the Global Subscription Server. |
| ***x* Kbytes per second** (field) | Defines the maximum data quantity value when **Enable Bandwidth Throttling** is selected (in Kbytes). |
| **Retry Limit** (field) | The maximum number of times Lumension EMSS attempts to reestablish communication with the GSS if the first attempt fails. |
| **Retry Wait** (field) | The number of seconds between retries. |
| **Connect Timeout** (field) | The number of seconds before a connection attempt is considered unsuccessful. |
| **Command Timeout** (field) | The number of seconds of inactivity before a command is considered unsuccessful. |

# Working with Subscription Updates

You can configure how the Lumension Endpoint Management and Security Suite server receives subscription updates from the Global Subscription Server by using the ***Subscription Updates*** page.


- *Replicating* on page 60
- *Editing the Communication Interval* on page 60
- *Restarting the Subscription Service* on page 62


## Replicating

Although the Lumension Endpoint Management and Security Suite regularly replicates with the Global Subscription Server automatically, you can manually perform replication should you need updates before the next scheduled automatic replication.

You can perform manual replications from the ***Subscriptions Updates*** page.

1. Select **Tools** > **Subscription Updates**.
2. Click **Update Now**.

   **Step Result:** A notification dialog opens.

3. Acknowledge the replication by clicking **OK**.

**Result:** Replication begins immediately. All license changes since the last replication are retrieved from the Global Subscription Server. This process may take several minutes, and no Discover Applicable Update tasks will run during the process.

## Editing the Communication Interval

Edit the communication interval to control when the Lumension Endpoint Management and Security Suite server downloads license data from the Global Subscription Server.

Edit the communication interval from the ***Subscription Updates*** page.

1. Select **Tools** > **Subscription Updates**.

   **Step Result:** The ***Subscription Updates*** page opens.

2. Select a time from the **Communication Interval** list located in the **Subscription Service Information** area. This list includes a value for every half-hour.
3. Click **Save**.

**Result:** The selected communication interval is saved. Your Lumension Endpoint Management and Security Suite server will replicate with the Global Subscription Server at the selected time.

## Configuring the Service Tab

Configuring the ***Service*** tab defines communication, proxy, and log settings pertaining to the Lumension Endpoint Management and Security Suite (Lumension EMSS) server and Global Subscription Server (GSS) communication.

Configure the ***Service*** tab from the ***Subscription Service Configuration*** dialog. Access this dialog from the ***Subscription Updates*** page.

1. Select **Tools** > **Subscription Updates**.
2. Click **Configure...**.

   **Step Result:** The ***Subscription Service Configuration*** dialog opens.
3. Ensure the ***Service*** tab is selected.
4. If using a proxy for communication between Lumension EMSS and the GSS, type the applicable information in the following fields.

| Field | Description |
|---|---|
| **Address** | The IP address or name of the proxy used for communication between Lumension EMSS and the GSS. |
| **Port** | The proxy port used for communication between Lumension EMSS and the GSS. |

5. If using a proxy that requires authentication, select the **Authenticated** check box and type the applicable information in the following fields.

| Field | Description |
|---|---|
| **User Name** | A user name that will authenticate with the proxy. |
| **Password** | The password associated with the user name. |
| **Confirm Password** | The password retyped. |

6. From the **Logging Level** list, select a logging level.

   Select from the following options.

| Option | Description |
|---|---|
| **Debug** | Logs errors, warnings, system actions, and debugging information.<br>**Note:** This logging level is the most comprehensive logging level. It should only be used for troubleshooting purposes due to the large logging files it produces and increased replication overhead it causes. |
| **Information** | Logs errors, warnings, and system actions. |
| **Warning** | Logs errors and warnings. |
| **Error** | Logs only errors. |

7. To limit the maximum data quantity during communication between Lumension EMSS and the GSS, select the **Enable Bandwidth Throttling** check box.
   a) Type the maximum number of kilobytes permitted per second in the ***X*** **Kbytes per second** field.

8. If desired, edit the following fields.

| Field Name | Description |
|---|---|
| **Retry Limit** | The maximum number of times Lumension EMSS attempts to reestablish communication with the GSS if the first attempt fails. |
| **Retry Wait** | The number of seconds between retries. |
| **Connect Timeout** | The number of seconds before a connection attempt is considered unsuccessful. |
| **Command Timeout** | The number of seconds of inactivity before a command is considered unsuccessful. |

**Note:** Under most network conditions, these fields do not require editing.

9. Click **Save**.

**Result:** Your edits are saved. These edits will take effect the next time Lumension EMSS communicates with the GSS.

### Restarting the Subscription Service

If the subscription service is stopped or needs restarting, it can be restarted within the Lumension Endpoint Management and Security Suite Web console.

You can restart the subscription service from the ***Subscription Service Configuration*** dialog ***Service*** tab.

1. Select **Tools** > **Subscription Updates**.
2. Click **Configure...**.

   **Step Result:** The ***Subscription Service Configuration*** dialog opens.

3. Ensure the ***Service*** tab is selected.
4. Click **Restart**.
5. Acknowledge the notification by clicking **OK**.

**Result:** The subscription service is restarted on the Lumension Endpoint Management and Security Suite server.

## The Email Notifications Page

You can configure Lumension Endpoint Management and Security Suite (Lumension EMSS) to send email notifications when certain system events occur. Configure email notifications from the ***Email Notifications*** page. Configuring Lumension EMSS to send you email notifications alerts you to system features that require administration.

You can configure email notification settings, define alert types, and set alert settings. Enter the email addresses that you want to receive notifications, and then select the alert types that you want each email address to receive.

You can enter an unlimited number of email addresses. Also use this page to define alert thresholds, which are data values that initiate email notifications.

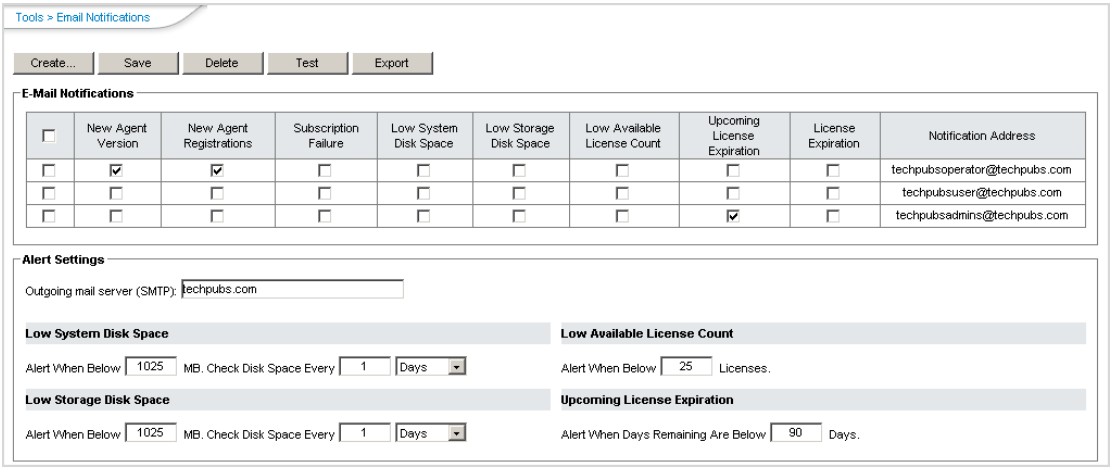



Figure 27: Email Notifications Page

## Viewing the Email Notifications Page

Navigate to ***Email Notification*** to define email addresses for notification alerts.

You can access this page at any time from the navigation menu.

1. Select **Tools** > **Email Notifications**.
2. View the email notifications.

## Email Notification Page Buttons

These buttons let you use functions available on the ***Email Notification*** page.

The following table describes each button function.

Table 33: Email Notification Page Buttons

| Button | Function |
|---|---|
| **Create...** | Creates a new email notification entry in **Email Notifications**. For additional information, refer to *Creating Email Notification Addresses* on page 68. |
| **Save** | Saves the changes made in **Email Notifications**. For additional information, refer to the following topics:<br>• *Creating Email Notification Addresses* on page 68<br>• *Editing Email Notification Addresses* on page 69 |
| **Delete** | Deletes the selected entry from **Email Notifications**. For additional information, refer to *Deleting Email Notification Addresses* on page 69. |
| **Test** | Sends a test email message to the selected email address(es). For additional information, refer to *Testing Email Notifications* on page 70. |

| Button | Function |
|---|---|
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br><br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |

## The Email Notifications Table

This table lists the email addresses that receive system alerts. You can also use this table to define a limitless number of addresses. The alert types sent to each email address can be customized.

The following table describes **Email Notifications**.

Table 34: E-Mail Notification Table

| Column | Description |
|---|---|
| **New Agent Version** | Alerts when a new version of the Lumension Endpoint Management and Security Suite (Lumension EMSS) agent becomes available for installation. |
| **New Agent Registrations** | Alerts when an agent registers with Lumension EMSS. |
| **Subscription Failure** | Alerts when any subscription task (download) fails. |
| **Low System Disk Space** | Alerts when the available system drive space on the Lumension EMSS Server falls below the defined minimum. |
| **Low Storage Disk Space** | Alerts when the available storage space on the drive where content is stored falls below the defined minimum. |
| **Low Available License Count** | Alerts when the number of licenses available to the Lumension EMSS falls below the defined minimum. |
| **Upcoming License Expiration** | Alerts when licenses will expire within the defined time frame. |
| **License Expiration** | Alerts when a license expires. |
| **Notification Address** | Lists the email address that receives alert notifications. Lumension EMSS does not validate the address. |
| **Note:** Option check boxes only appear in **Email** notifications after you create an email notifications entry. | |

For additional information about creating email notifications, refer to *Working with Email Notifications* on page 67.

## Alert Settings

*Alert settings* are user-defined values that trigger notification emails. These values are defined from the **Alert Settings** options. Edit these values to suit your network environment. Settings are available for system disk space, storage disk space, and license information.

The following table describes the **Alert Settings** options.

Table 35: Alert Settings Options

| Option | Definition |
|---|---|
| **Outgoing Mail Server (SMTP)**<br>(Field) | The mail host used by Lumension Endpoint Management and Security Suite (Lumension EMSS) for sending email messages.<br>**Note:** The **Outgoing Mail Server (SMTP)** is not an alert value setting. However, completion of this field with your network's valid SMTP server is required for addresses listed in the **Email Notifications** table to receive alerts. |
| **Low System Disk Space** | Defines the threshold that initiates email notifications due to low system disk space. Define the following options:<br>**Alert When Below *x* MB (field)** — Defines the level of system disk space that Lumension EMSS must drop below before an alert is generated (1-9,999 MBs [9.765 GB]).<br>**Check Disk Every *x Interval* (field and list)** — Defines the interval between **Low System Disk Space** threshold checks. This interval is defined in minutes, hours, or days (1-99). |
| **Low Storage Disk Space** | Defines the threshold that initiates email notifications due to low storage disk space. Define the following options:<br>**Alert When Below *x* MB (field)** — Defines the level of storage disk space that Lumension EMSS must drop below before an alert is generated (1-9,999 MBs [9.765 GB]).<br>**Check Disk Every *x Interval* (field and list)** — Defines the interval between **Low Storage Disk Space** threshold checks. This interval is defined in minutes, hours, or days (1-99). |

| Option | Definition | |
|---|---|---|
| **Low Available License Count** | Defines the threshold that initiates email notifications due to low available license count. Define the following option: | |
| | **Alert for any Module That Falls Below *x* Licenses (field)** | Defines the number of available licenses that Lumension EMSS must drop below before an alert is generated (1-999). |
| | **While License Count Remains Low, Send a Reminder E-mail Every *x* Days (check box and field)** | Defines if an alert is sent and the interval in days (1-99). |
| **Upcoming License Expiration** | Defines the threshold that initiates email notifications due to upcoming license expiration. Define the following option: | |
| | **Alert for any License That Will Expire Within *x* Days (field)** | Defines the number of days before an alert is generated due to upcoming license expiration (1-99). |
| | **While Licenses Aren't Renewed After This Alert, Send a Reminder E-mail Every *x* Days (check box and field)** | Defines if an alert is sent and the interval in days (1-99). |

Thresholds define the value that initiate email notifications, but not email notifications themselves. Email notifications are sent following Discover Applicable Updates (DAU) tasks that find values below the defined thresholds.

For additional information on defining alert thresholds, refer to *Defining Alert Settings* on page 67.

## RSS Feed

You can receive additional security notifications via a Lumension RSS feed. A **Real Simple Syndication (RSS)** feed is a notification method to start the import and export process.

To receive notifications to start the import and export process use an RSS reader. Subscribe to the following Lumension feed: *http://gssnews.lumension.com/news/default.aspx?oem=Lumension*.

**Note:** The RSS feed transmits Global Subscription Server notifications. It is not a method of receiving system specific notifications (such as email notifications).

# Working with Email Notifications

From the ***Email Notifications*** page, you can define the email addresses that receive notifications. You can also define the events and values that trigger notification emails.


- *Defining Alert Settings* on page 67
- *Creating Email Notification Addresses* on page 68
- *Editing Email Notification Addresses* on page 69
- *Deleting Email Notification Addresses* on page 69
- *Testing Email Notifications* on page 70


## Defining Alert Settings

Alert settings are values that trigger the Lumension Endpoint Management and Security Suite server to send email notifications. Define these values for preventive maintenance purposes.

Define alert settings from the ***Email Notifications*** page.

1. Select **Tools** > **Email Notifications**.
2. In the **Outgoing Mail Server (SMTP), type (or edit) the name of your outgoing mail server.**

   Type the name in the following format: `mail.company.com`.

   **Note:** The outgoing mail server is not an alert setting value, but is necessary to define email notification addresses.

3. Define the **Low System Disk Space** options.

   This alert setting defines when email notifications are send due to low system disk space.

   a) Type a value in the **Alert When Below *x* MB** field (1-9999).
   b) Type a value in the **Check Disk Space Every *x Interval*** field (1-99).
   c) Select an interval from the **Check Disk Space Every *x Interval*** list (**Minute(s)**, **Hours**, **Days**).

4. Define the **Low Storage Disk Space** options.

   This alert setting defines when email notifications are sent due to low storage disk space.

   a) Type a value in the **Alert When Below *x* MB** field (1-9999).
   b) Type a value in the **Check Disk Space Every *x Interval*** field (1-99).
   c) Select an interval from the **Check Disk Space Every *x Interval*** list (**Minute(s)**, **Hours**, **Days**).

5. Define the **Low Available License Count** options.

   This alert setting defines the number of available licenses that Lumension Endpoint Management and Security Suite must drop below before an email notification is generated.

   a) Type a value in the **Alert for any Module That Falls *x* Licenses** field. (1-9999).
   b) If applicable, select the check box and type a value in the **While License Count Remains Low, Send a Reminder Email Every *x Interval*** field (1-99).

6. Define the **Upcoming License Expiration** options.
   This alert setting defines the number of days before an email notification is generated to upcoming license expiration.
   a) Type a value in the **Alert for any Licenses That Will Fall Within *x* Days** field (1-99).
   b) If applicable, select the check box and type a value in the **While Licenses Aren't Renewed After This Alert, Send a Reminder Email Every *x Interval*** field. (1-99).
7. Click **Save**.

**Result:** Your alert setting values are saved.

## Creating Email Notification Addresses

You can configure Lumension Endpoint Management and Security Suite (Lumension EMSS) to send emails to defined email addresses when certain system events occur. Define email notification recipients for preventative maintenance and administrative purposes.

**Prerequisites:**

Complete *Defining Alert Settings* on page 67.

Define email notification recipients from the ***Email Notifications*** page.

1. Select **Tools** > **Email Notifications**.
2. Click **Create...**.

   **Step Result:** A new row displays in the **Email Notifications** table.
3. Type an email address in the **Notifcation Address** field of the new row.

   **Note:** Lumension EMSS does not validate email addresses.
4. Select the check boxes associated with the email notifications that you want the email address to receive.
   The following table describes each email notification.

| Notification | Description |
|---|---|
| **New Agent Version** | Alerts when a new version of the agent becomes available for installation. |
| **New Agent Registrations** | Alerts when an agent registers with the Lumension EMSS Server. |
| **Subscription Failure** | Alerts when any subscription task (download) fails. |
| **Low System Disk Space** | Alerts when the available system drive space on the Lumension EMSS server falls below the defined minimum. |
| **Low Storage Disk Space** | Alerts when the available storage space on the drive where content is stored falls below the defined minimum. |
| **Low Available License Count** | Alerts when the number of licenses available to Lumension EMSS fall below the defined minimum. |
| **Upcoming License Expiration** | Alerts when licenses will expire within the defined time frame. |

| Notification | Description |
|---|---|
| **License Expiration** | Alerts when a license expires. |

5. Click **Save**.

**Result:** The email notification address and the selected notifications are saved. The address will receive a notification when the applicable system events occur.

## Editing Email Notification Addresses

After an email notification address is created, you can edit the email address itself, or you can change notification types it receives.

Edit email notification addresses from the ***Email Notifications*** page.

1. Select **Tools** > **Email Notifications**.

   **Step Result:** The ***Email Notifications*** page opens.

2. From the **Notification Address** column, edit the desired email address field(s).
3. Select or clear the desired notification type check boxes.
   The following table describes each notification type.

| Notification | Description |
|---|---|
| **New Agent Version** | Alerts when a new version of the agent becomes available for installation. |
| **New Agent Registrations** | Alerts when an agent registers with the Lumension EMSS Server. |
| **Subscription Failure** | Alerts when any subscription task (download) fails. |
| **Low System Disk Space** | Alerts when the available system drive space on the Lumension EMSS server falls below the defined minimum. |
| **Low Storage Disk Space** | Alerts when the available storage space on the drive where content is stored falls below the defined minimum. |
| **Low Available License Count** | Alerts when the number of licenses available to Lumension EMSS fall below the defined minimum. |
| **Upcoming License Expiration** | Alerts when licenses will expire within the defined time frame. |
| **License Expiration** | Alerts when a license expires. |

4. Click **Save**.

## Deleting Email Notification Addresses

Delete email notification address that no longer need notification of system events.

Delete email notification recipients from the ***Email Notifications*** page.

1. Select **Tools** > **Email Notifications**.

   **Step Result:** The ***Email Notifications*** page opens.

2. Select the check box(es) associated with the notification address(es) that you want to delete.
3. Click **Delete**.

   **Step Result:** The ***Message from webpage*** opens indicating the selected recipients have been removed.

4. Click **OK**.

**Result:** The notification address is deleted. The address will no longer receive notification emails.

### Exporting Email Notification Data

You can export email notification data to a comma separated value (`.csv`) file for reporting and analytical purposes.

All data on the page is exported. To export email notification data, select **Tools** > **Email Notifications** and click **Export**. For additional information, refer to *Exporting Data* on page 37.

### Testing Email Notifications

Testing email notifications ensures that defined email addresses and Lumension Endpoint Management and Security Suite are properly configured for alerts. If a test fails, you should first verify that the email address is typed correctly in the **Email Notifications** table. If it is, you should then examine email and Lumension Endpoint Management and Security Suite settings.

**Prerequisites:**

An email address must be added to the **Email Notifications** table.

Test email notifications from the ***Email Notifications*** page.

1. Select **Tools** > **Email Notifications**.
2. From **Email Notifications**, select the check box(es) associated with the email address(es) you want to test.
3. Click **Test**.

**Result:** A notification informs you that the test email was sent. Acknowledge the notification by clicking **OK**. Access the applicable email address to ensure the notification was successful.

## The Options Page

Within Lumension Endpoint Management and Security Suite, you can control a number of default settings from the ***Options*** page: user interface options, agent options, and so on. While most of these options can be

edited when using product functions, configuring default settings saves time and effort when using these product functions.

The ***Options*** page contains the following tabs, which contain options related to their labels:

- *The General Tab* on page 72
- *The Agents Tab* on page 74

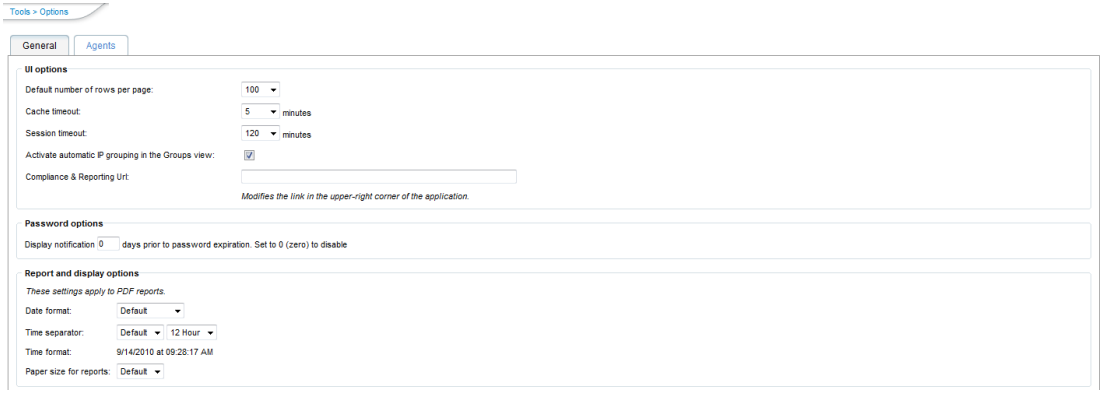



Figure 28: Options Page

## The Options Page Buttons

The ***Options*** page contains several buttons that are common to each of its tabs. These buttons share similar functions to buttons commonly seen on page toolbars.

The following table describes the ***Option*** page button functions.

| Button | Function |
|---|---|
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br><br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |
| **Reset** | Cancels any edits made to the options since the tab was loaded. |
| **Save** | Saves the tab option settings (if any edits were made). You must click this button to implement your edits. |

## Viewing the Options Page

Navigating to the ***Options*** page lets you view and edit default values for various options, which save you time when using product features.

You can reach this page at any time from the navigation menu.

1. Select **Tools** > **Options**.
2. Select the desired tab:

- The ***General*** tab
- The ***Agents*** tab

3. If desired, complete a task listed in *Working with Options* on page 78.

## The General Tab

Default settings for user interface options, password options, and report and display options are controlled from the ***General*** tab. The options available on this page are generalized and are not closely related.

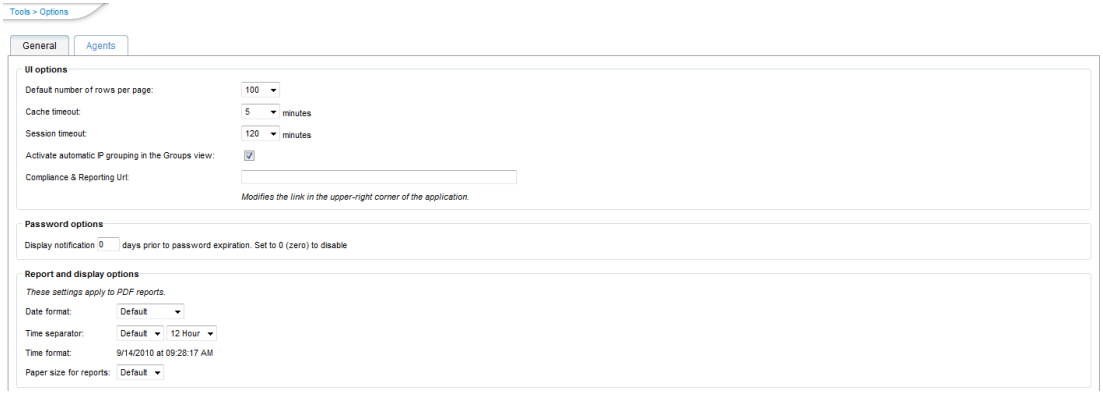



Figure 29: General Tab

### UI Options

With these options, you can control user interface features according to your preferences.

Select from lists and check boxes to configure **UI options**.

The following table describes the available options.

Table 36: UI Options

| Option | Description |
|---|---|
| **Default number of rows per page** (list) | Defines the default number of rows that display in list pages (**25**, **50**, **100**, **200**, **500**). |
| **Cache timeout** (list) | Defines the maximum number of minutes data is held in the memory before it needs to be reloaded from the database (**5**, **10**, **15**, **20**, **30**). |
| **Session timeout** (list) | Defines the number of minutes before a repeat login is required due to inactivity (**20**, **40**, **60**, **80**, **100**, **120**). |
| **Activate automatic IP grouping in the Groups view** (checkbox) | Creates groups organized by IP address in the ***Groups*** page **Group Browser** named **IP Collection**.<br>**Note:** Only agent versions 6.4 or later appear in these groups. |

| Option | Description |
|---|---|
| **Compliance & Reporting URL** (field) | Modifies the link in the product header. |

## Password Options

The single **Password option** lets you configure Lumension Endpoint Management and Security Suite to display a notification warning you of upcoming password expirations. If your user account does not have a password expiration, this setting is disregarded. When this option is enabled, a password expiration warning displays when you log in to the Web console.

Complete the field to configure the options.

The following table describes the available **Password option**.

Table 37: Password Options

| Option | Description |
|---|---|
| **Display notification *x* days prior to password expiration.** (field) | Defines the number of days prior to a required password change (as controlled by Windows) that a notification displays. A value of `0` disables the notification. |

## Report and Display Options

These options control date, time, and paper formatting for reports generated in Lumension Endpoint Management and Security Suite. Modify date and time settings according to how your enterprise formats date and time. Modify paper settings according the paper types your enterprises uses for printing.

**Note:** These options apply only to reports in a PDF format.

Select from the lists to configure the options.

The following table describes the available **Report and display options**.

Table 38: Report and Display Options

| Option | Description |
|---|---|
| **Date Format** (list) | Defines the date format displayed in text-based and graphical reports. Select from the following options:<br>• **Default** (mm/dd/yyyy)<br>• **MM/dd/yyyy**<br>• **dd/MM/yyyy**<br>• **yyyy-MM-dd**<br>• **dd.MM.yyyy**<br>• **dd-MM-yyyy**<br>• **yyyy/MM/dd** |

| Option | Description |
|---|---|
| **Time Separator** (lists) | Defines the character used to separate hours, minutes, and seconds in reports. Select from the following options:<br>• **Default** (the current character in use)<br>• **Colon (:)**<br>• **Period (.)**<br>This option also defines the time notation used in reports. Select from the following options:<br>• **12 Hour**<br>• **24 Hour** |
| **Time Format** (field) | Displays the selected **Date Format** punctuated by the selected **Time Separator**. This field refreshes as you select different **Report and display options**. |
| **Paper Size for Reports** (list) | Defines how reports are formatted for printing. Select from the following options:<br>• **Default** (the currently saved formatting style)<br>• **Letter**<br>• **A4** |

## The Agents Tab

This tab controls aspects related to agent management jobs and agent-to-server communication. Editing options related to agent management jobs sets default values for agent management jobs.

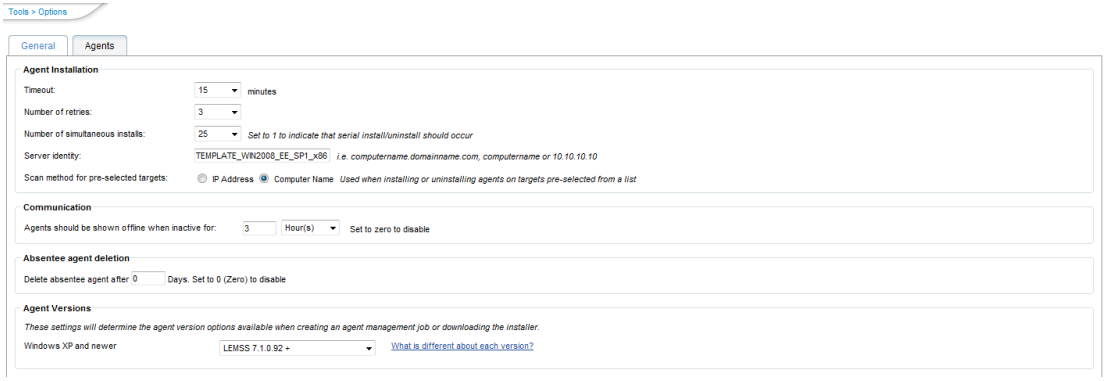

Tools > Options
General
Agents
Agent Installation
Timeout:
15
minutes
Number of retries:
3
Number of simultaneous installs:
25
Set to 1 to indicate that serial install/uninstall should occur
Server identity:
TEMPLATE_WIN2008_EE_SP1_x86
i.e. computername.domainname.com, computername or 10.10.10.10
Scan method for pre-selected targets:
IP Address
Computer Name
Used when installing or uninstalling agents on targets pre-selected from a list
Communication
Agents should be shown offline when inactive for:
3
Hour(s)
Set to zero to disable
Absentee agent deletion
Delete absentee agent after 0 Days. Set to 0 (Zero) to disable
Agent Versions
These settings will determine the agent version options available when creating an agent management job or downloading the installer.
Windows XP and newer
LEMSS 7.1.0.92 +
What is different about each version?

Figure 30: Agents Tab

## Agent Installation

These options define default installation values for agent management jobs. When configuring agent management jobs, these settings can be changed. Adjusting these settings to frequently used values can save effort during agent management job configuration.

Use **Agent Installation** options to define the default settings for the ***Agent Settings*** page in the ***Schedule Agent Management Job Wizard***. Complete the field and select from the lists to define the options.

Table 39: Agent Installation Options

| Agent Installation Option | Description |
|---|---|
| **Timeout**<br>(drop-down list) | Defines the default number of minutes before an agent installation job terminates due to non-responsive status (0-30). |
| **Number of retries**<br>(drop-down list) | Defines the default number of attempts an agent installation will retry if initial and subsequent installations fails (1-10). |
| **Number of simultaneous installs**<br>(drop-down list) | Defines the default maximum number of agents that can be installed or un-installed simultaneously during an agent management job (1-25). A setting of `1` indicates that serial install/uninstalls should occur. |
| **Server identity**<br>(field) | Defines the default text entered in the **Server Identity** field during agent installation jobs. **Server Identity** is the name agents list as their Lumension Endpoint Management and Security Suite server. |
| **Scan method for pre-selected targets**<br>(radio buttons) | Defines how endpoints pre-selected from a page list are added to a job's **targets** list (discovery scan or agent management) after launching a job configuration dialog. The options are:<br>**IP Address** — Adds the selected endpoint to a job's target list using its IP address.<br>**Computer Name** — Adds the selected endpoint to a job's target list using its endpoint name. |

## Communication

These options define how Lumension Endpoint Management and Security Suite recognizes the agent. Modifying the **Agents should be shown offline when inactive for** option changes the time duration before Lumension Endpoint Management and Security Suite considers an agent offline. Modifying the **Stand alone Patch agent uniqueness based on** option changes how the server validates agents during communication.

Complete the fields, select from the list, and select a radio button to configure the options.

The following table describes **Communication** options.

Table 40: Communication Options

| Option | Description | |
|---|---|---|
| **Agents should be shown offline when inactive for** (field and list) | Defines the time period (in minutes, hours, or days) before an agent is considered offline because it has not checked in with Lumension EMSS. Disabled and un-installed agents are not considered offline. A value of *0* disables this option. | |
| **Stand alone Patch agent uniqueness based on** (radio buttons) | Defines how the server identifies patch agents during communication (Patch and Remediation only). The options are: | |
| | **Endpoint name** | Configures the server to identify agents using the NetBIOS name of the endpoint. Select this option in environments that do not contain multiple instances of a single NetBIOS name, as it reduces administrative maintenance in the event that an endpoint needs to be re-imaged. This option is selected by default. |
| | **Instance** | Configures the server to identify agents using a unique number. Select this option in larger network environments where multiple instances of a single NetBIOS exist. This option prevents communication errors that may occur if multiple agents share a single NetBIOS name. |

## Absentee Agent Deletion

Sporadically, a Lumension Endpoint Management and Security Suite Agent will cease communication with the Lumension Endpoint Management and Security Suite server. By defining the **Absentee Agent Deletion** option, you are configuring Lumension Endpoint Management and Security Suite to automatically delete uncommunicative agents.

Complete the field to configure the option.

The following table describes the **Absentee Agent Deletion** option.

Table 41: Absentee Agent Deletion Option

| Option | Description |
|---|---|
| **Delete absentee agent after *x* days.** | Removes an uncommunicative agent after the defined time period (days). A value of *0* disables this function. |

## Agent Versions

The Lumension Endpoint Management and Security Suite agent comes in multiple versions across multiple platforms. By defining **Agent Version** options, you can restrict which versions are available to install, upgrade, or overwrite. You can restrict available versions for each platform. These options are useful for maintaining agent uniformity across your network.

To define the options, select from the lists.

The following table describes each **Agent Version** option.

Table 42: Agent Version Options

| Option | Description |
|---|---|
| **Windows XP and newer agent version**<br>(list) | Defines which agent versions are available for installation on endpoints running Windows XP or a newer Windows-based operating system when working with the following system dialogs:<br>• The ***Manage Agent Versions*** Dialog<br>• The ***Download Agent Installers*** Dialog<br>• The ***Install Agents Wizard*** |
| When selecting agent version options, remember the following information:<br>• **Newest Available** means only the latest agent version is available for installation.<br>**Note:** This option only defines which agent version is available when working with the ***Manage Agent Versions*** dialog, the ***Download Agent Installers*** dialog, or the ***Install Agents Wizard***. It does not automatically install newly released agent versions on network endpoints. To ensure the newest agent version in stalled on network endpoints, you must manually define the latest version. For additional information, refer to *Defining the Endpoint Agent Version* on page 166.<br>• ***Agent Version* only** list items mean only that agent version is available for installation.<br>• ***Agent Version* +** list items mean that agent version and all version that supersede it are available for installation. | |

### The Agent Version Detail Dialog

This dialog describes the various agent versions. It also lists system requirements, applicable notes, and recent changes.

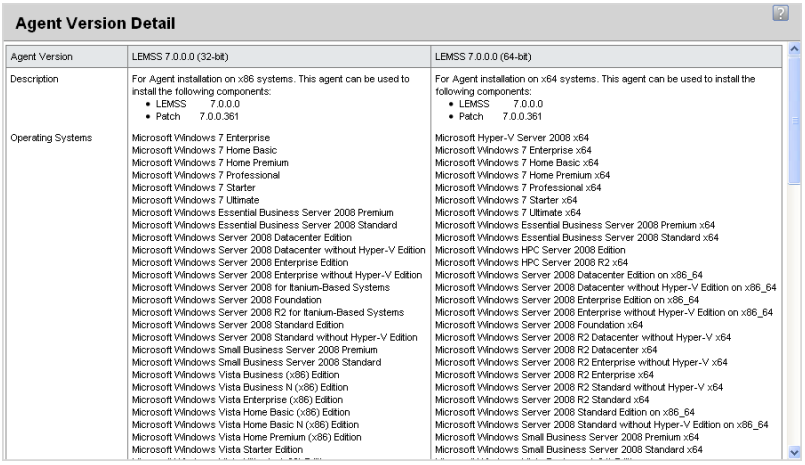

Agent Version Detail
Agent Version
LEMSS 7.0.0.0 (32-bit)
LEMSS 7.0.0.0 (64-bit)
Description
For Agent installation on x86 systems. This agent can be used to install the following components:
• LEMSS 7.0.0.0
• Patch 7.0.0.361
For Agent installation on x64 systems. This agent can be used to install the following components:
• LEMSS 7.0.0.0
• Patch 7.0.0.361
Operating Systems
Microsoft Windows 7 Enterprise
Microsoft Windows 7 Home Basic
Microsoft Windows 7 Home Premium
Microsoft Windows 7 Professional
Microsoft Windows 7 Starter
Microsoft Windows 7 Ultimate
Microsoft Windows Essential Business Server 2008 Premium
Microsoft Windows Essential Business Server 2008 Standard
Microsoft Windows Server 2008 Datacenter Edition
Microsoft Windows Server 2008 Datacenter without Hyper-V Edition
Microsoft Windows Server 2008 Enterprise Edition
Microsoft Windows Server 2008 Enterprise without Hyper-V Edition
Microsoft Windows Server 2008 for Itanium-Based Systems
Microsoft Windows Server 2008 Foundation
Microsoft Windows Server 2008 R2 for Itanium-Based Systems
Microsoft Windows Server 2008 Standard Edition
Microsoft Windows Server 2008 Standard without Hyper-V Edition
Microsoft Windows Small Business Server 2008 Premium
Microsoft Windows Small Business Server 2008 Standard
Microsoft Windows Vista Business (x86) Edition
Microsoft Windows Vista Business N (x86) Edition
Microsoft Windows Vista Enterprise (x86) Edition
Microsoft Windows Vista Home Basic (x86) Edition
Microsoft Windows Vista Home Basic N (x86) Edition
Microsoft Windows Vista Home Premium (x86) Edition
Microsoft Windows Vista Starter Edition
Microsoft Hyper-V Server 2008 x64
Microsoft Windows 7 Enterprise x64
Microsoft Windows 7 Home Basic x64
Microsoft Windows 7 Home Premium x64
Microsoft Windows 7 Professional x64
Microsoft Windows 7 Starter x64
Microsoft Windows 7 Ultimate x64
Microsoft Windows Essential Business Server 2008 Premium x64
Microsoft Windows Essential Business Server 2008 Standard x64
Microsoft Windows HPC Server 2008 Edition
Microsoft Windows HPC Server 2008 R2 x64
Microsoft Windows Server 2008 Datacenter Edition on x86_64
Microsoft Windows Server 2008 Datacenter without Hyper-V Edition on x86_64
Microsoft Windows Server 2008 Enterprise Edition on x86_64
Microsoft Windows Server 2008 Enterprise without Hyper-V Edition on x86_64
Microsoft Windows Server 2008 Foundation x64
Microsoft Windows Server 2008 R2 Datacenter without Hyper-V x64
Microsoft Windows Server 2008 R2 Datacenter x64
Microsoft Windows Server 2008 R2 Enterprise without Hyper-V x64
Microsoft Windows Server 2008 R2 Enterprise x64
Microsoft Windows Server 2008 R2 Standard without Hyper-V x64
Microsoft Windows Server 2008 R2 Standard x64
Microsoft Windows Server 2008 Standard Edition on x86_64
Microsoft Windows Server 2008 Standard without Hyper-V Edition on x86_64
Microsoft Windows Small Business Server 2008 Premium x64
Microsoft Windows Small Business Server 2008 Standard x64

Figure 31: Agent Version Detail Dialog

To access this dialog, click the **What is different about each version?** link on the ***Agents*** tab.

The following table describes each field in the ***Agent Version Detail*** dialog.

| Field | Description |
|---|---|
| **Agent Version** | The agent name and version number. |
| **Description** | A description of the applicable agent. This field also lists the components that are installed with the agent. |
| **Operating Systems** | The operating systems that are supported by the applicable agent. |
| **System Requirements** | The system requirements to install the agent on a target endpoint. |
| **Installation Notes** | The information notes pertaining to installation of the agent. |
| **Changes** | The changes made to the applicable agent since its previous release. |

## Working with Options

From each ***Options*** page tab, you can define default behavior for different Lumension Endpoint Management and Security Suite features.


- *Configuring the General Tab* on page 79
- *Configuring the Agents Tab* on page 80
- *Exporting Option Data* on page 83

## Configuring the General Tab

Configure this tab to define how user interface, password, and report display options behave.

Configure the ***General*** tab from the ***Options*** page.

1. Select **Tools** > **Options**.

   **Step Result:** The ***Options*** page opens.

2. Ensure the ***General*** tab is selected.
3. Define the **UI options**.

   These options define general user interface behavior.

   a) Select a value from the **Default number of rows page** list (**25**, **50**, **100**, **200**, **500**).

   This option defines the default number of rows that display in list pages.

   b) Select a value from the **Cache timeout** list (**5**, **10**, **15**, **20**, **30**).

   This option defines the maximum number of minutes data is held in the memory before it needs to be reloaded from the database.

   c) Select a value from the **Session timout** list (**20**, **40**, **60**, **80**, **100**).

   This option defines the number of minutes before a repeat login is required due to inactivity.

   d) Select or clear the **Activate automatic IP grouping in the Groups view** check box.

   This option creates groups organized by IP address in the Groups page Group Browser named IP Collection.

   e) If desired, edit the **Compliance & Report URL** field in the following format: `http(s)://www.website.com`.

   This field controls what web address the product header links you to. Lumension recommends using the link to direct you to your reporting and compliance Web site.

4. Define the **Password options**.

   This option defines the number of days prior to a required password change (as controlled by Windows) that a notification displays. Type a value in the **Display notification *x* days prior to password expiration** field. A value of `0` disables password expiration.

5. Define the **Report and display options**.

   These options control formatting options for PDF reports. Perform the step(s) required to define each option.

**Note:** The **Default** item available in each **Report and display options** returns the applicable option to the last saved value.

| Option | Step(s) |
|---|---|
| **Date format** | This option defines the date format displayed in text-based and graphical reports.<br>Select a value from the **Date format** list. |

| Option | Step(s) |
|---|---|
| **Time seperator** | This option defines the character used to separate hours, minutes, and seconds in reports. This option also defines the time notation used in reports.<br>**1.** Select a character from the first **Time separator** list (colon [:] or period [.]).<br>**2.** Select a value from the second **Time separator** list (**12 Hour** or **24 Hour**). |
| **Paper size for report** | This option Defines how reports are formatted for printing.<br>Select a value from the **Paper size for reports** list (`Letter` or `A4`). |

6. Click **Save**.

**Result:** The ***General*** tab configuration is saved.

## Configuring the Agents Tab

Configure this tab to define default behavior for agent installation, communication, discover applicable update tasks, ISAPI communication, and agent versions.

Configure the ***Agents*** tab from the ***Options*** page.

1. Select **Tools** > **Options**.

   **Step Result:** The ***Options*** page opens.

2. Select the ***Agents*** tab.
3. Define the **Agent Installation** options.

   These options define the default behavior of agent management jobs.

   a) Select a value from the **Timeout** list (**1**-**30** minutes).

   This option defines the default number of minutes before an agent installation job terminates due to non-responsive status

   b) Select a value from the **Number of retries** list (**1**-**10**).

   This option defines the default number of attempts an agent installation will retry if initial and subsequent installations fails

   c) Select a value from the **Number of simultaneous installs** list (**1**-**25**).

   This option defines the default maximum number of agents that can be installed or un-installed simultaneously during an agent management job. A value of **1** indicates that serial installs and uninstalls should occur.

d) Type a value in the **Server identity** field.

This field defines the default text entered in the **Server Identity** field during agent installation jobs. Server Identity is the name agents list as their Lumension Endpoint Management and Security Suite server. The server identity should be typed in one of the following formats:

- `computername.domainname.com`
- `computername`
- `10.10.10.10`

e) Select a **Scan method for pre-selected targets** option:

These buttons define how endpoints pre-selected from a page list are added to a job's targets list (discovery scan or agent management) after launching a job configuration dialog. The options include:

- **IP Address**
- **Computer Name**

4. Define the **Communication** options.

To define these options, complete the following substeps.

a) Type a value in the **Agents should be shown offline when inactive for** field (**0**-**9999**).

This option defines the time period (in minutes, hours, or days) before an agent is considered offline because it has not checked in with Lumension EMSS. Disabled and un-installed agents are not considered offline. A value of *0* disables this option.

b) Select a value from the **Agents should be shown offline when inactive for** list.

Select from the following values:

- **Minute(s)**
- **Hour(s)**
- **Day(s)**

c) Select a **Stand alone Patch agent uniqueness based on** option.

These options define how the server identifies patch agents during communication (Patch and Remediation only). Select from the following options:

- **Endpoint name**
- **Instance**

5. Define the **Discover Applicable Updates (DAU) Options**.

These options determine whether registered agents perform a DAU task following a subscription replication or inventory change. Select or clear the following options:

- **DAU should be run after subscription replication**
- **DAU should be run after inventory change**

6. Define the **Absentee agent deletion** option.

This option defines when an uncommunicative agent after the defined time period (days). A value of *0* disables this function. Type a value in the **Delete absentee agent after *x* Days** field (**0**-**999**) Days. A value of `0` disables the option.

7. Define the **ISAPI communication** options.

| Option | Steps |
|---|---|
| **Concurrent agent limit** | This option defines the maximum number of threads used by Lumension EMSS.<br>To use the default option:<br>Select the **SQL default (64 threads)**.<br>To use a custom option:<br>1. Select the **Custom setting (5-256)** option.<br>2. Type a value in the ***x* threads** field (**5-256**). |
| **Connection timeout** | This option defines the time (in seconds) before an ISAPI thread expires (times out).<br>To use the default option:<br>Select the **Default (30 seconds)** option.<br>To use a custom option:<br>1. Select the **Custom setting (5 to 300 seconds) option**.<br>2. Type a value in the **seconds** field (**5-300**). |
| **Command timeout** | This option defines the time (in seconds) before an ISAPI command expires (times out).<br>To use the default option:<br>Select the **Default (60 seconds)** option.<br>To use a custom option:<br>1. Select the **Custom setting (5 to 900 seconds)** option.<br>2. Type a value in the **seconds** field (**5-900**). |

8. Define the **Agent Versions** options.

   These options define the agent versions that are available for installation during when working with the following system dialogs:

   - The ***Manage Agent Versions*** Dialog
   - The ***Download Agent Installers*** Dialog

- The ***Install Agents Wizard***

a) Select a value from the **Windows XP and newer agent version**.

Because the agent is updated regularly, **Agent Versions** option list values change frequently. Additionally, when selecting agent version options, remember the following information:

- **Newest Available** means only the latest agent version is available for installation.

  **Note:** This option only defines which agent version is available when working with the ***Manage Agent Versions*** dialog, the ***Download Agent Installers*** dialog, or the ***Install Agents Wizard***. It does not automatically install newly released agent versions on network endpoints. To ensure the newest agent version in stalled on network endpoints, you must manually define the latest version. For additional information, refer to *Defining the Endpoint Agent Version* on page 166.

- ***Agent Version* only** list items mean only that agent version is available for installation.
- ***Agent Version* +** list items mean that agent version and all version that supersede it are available for installation.

**9.** Click **Save**.

**Result:** The ***Agents*** tab configuration is saved.

## Exporting Option Data

To export the options settings that are listed on any ***Options*** page tab to a comma separated value (`.csv`) file, click the **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to *Exporting Data* on page 37.

# Chapter 4

# Licensing and Support

**In this chapter:**


- The Technical Support Page
- The Product Licensing Page


While using Lumension Endpoint Management and Security Suite (Lumension EMSS), you may need to request technical support or view information about your Lumension EMSS licenses.

Request technical support from the *The Technical Support Page* on page 86. From this page you can request technical support and review technical information about your Lumension EMSS Server.

View licensing information from the *The Product Licensing Page* on page 91. This page lists the Lumension EMSS modules you are licensed for.

# The Technical Support Page

Lumension offers a variety of technical support Web pages, as well as Web pages where you can give Lumension feedback for future product releases. You can access these pages from the **Technical Support** page.

This page also provides a variety of read-only system data pertaining to the Lumension Endpoint Management and Security Suite environment.

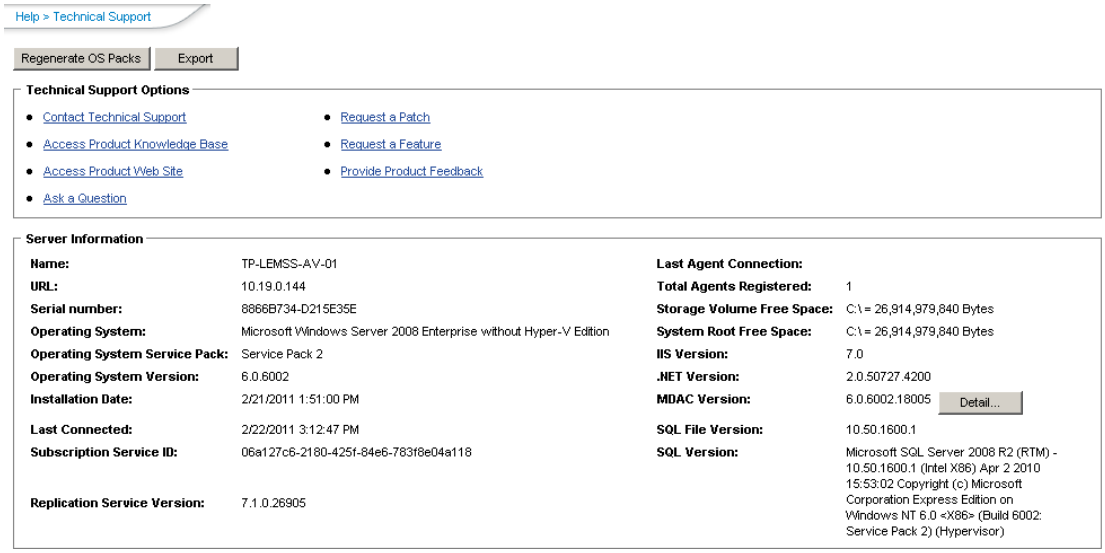

Help > Technical Support
Regenerate OS Packs
Export
Technical Support Options
Contact Technical Support
Access Product Knowledge Base
Access Product Web Site
Ask a Question
Request a Patch
Request a Feature
Provide Product Feedback
Server Information
Name: TP-LEMSS-AV-01
URL: 10.19.0.144
Serial number: 8866B734-D215E35E
Operating System: Microsoft Windows Server 2008 Enterprise without Hyper-V Edition
Operating System Service Pack: Service Pack 2
Operating System Version: 6.0.6002
Installation Date: 2/21/2011 1:51:00 PM
Last Connected: 2/22/2011 3:12:47 PM
Subscription Service ID: 06a127c6-2180-425f-84e6-783f8e04a118
Replication Service Version: 7.1.0.26905
Last Agent Connection:
Total Agents Registered: 1
Storage Volume Free Space: C:\ = 26,914,979,840 Bytes
System Root Free Space: C:\ = 26,914,979,840 Bytes
IIS Version: 7.0
.NET Version: 2.0.50727.4200
MDAC Version: 6.0.6002.18005
Detail...
SQL File Version: 10.50.1600.1
SQL Version: Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (Intel X86) Apr 2 2010 15:53:02 Copyright (c) Microsoft Corporation Express Edition on Windows NT 6.0 <X86> (Build 6002: Service Pack 2) (Hypervisor)

Figure 32: Technical Support Page

## Viewing the Technical Support Page

Navigate to this page to access out-of-program technical support pages.

You can access this page at any time from the navigation menu.

1. Select **Help** > **Technical Support**.
2. View the page.

## Technical Support Page Buttons

Click these buttons to use features available from the ***Technical Support*** page.

The following table describes each button.

Table 43: Technical Support Page Buttons

| Button | Function |
|---|---|
| **Regenerate OS Packs** | Regenerates and synchronizes the relevant information for each of the operating systems supported by Lumension Endpoint Management and Security Suite. For additional information, refer to *Regenerating OS Packs* on page 90. |

| Button | Function |
|---|---|
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |
| **Detail...** | Opens a dialog that displays a detailed list of Microsoft Directory Access Components product and file versions. For additional information, refer to *Regenerating OS Packs* on page 90. |

## Technical Support Options

Lumension provides access to various out-of-program technical support pages. Use these pages to communicate with Lumension. Click each link to open the applicable page in a new window.

The following table describes each link.

Table 44: Technical Support Options Links

| Link | Description |
|---|---|
| **Contact Technical Support** | Sends an email to technical support at *Lumension Support* (*patchlink.support@lumension.com*). |
| **Access Product Knowledge Base** | Accesses the knowledge base at *Lumension Support* (*http://support.lumension.com*). |
| **Access Product Web Site** | Accesses the *Lumension web site* (*http://www.lumension.com*). |
| **Ask a Question** | Sends a support question to Lumension via the *Lumension Customer Portal* (*http://portal.lumension.com/*). |
| **Request a Patch** | Sends a patch request to *Lumension Support* (*patchlink.support@lumension.com*). |
| **Request a Feature** | Sends a feature request to Lumension via the *Product Feedback and Feature Request Page* (*http://my.lumension.com/feedback.spring*). |
| **Provide Product Feedback** | Sends product input to Lumension via the *Product Feedback and Feature Request Page* (*http://my.lumension.com/feedback.spring*). |

## Server Information

These fields list general information regarding the Lumension Endpoint Management and Security Suite (Lumension EMSS) system.

The following table describes the **Server Information** fields.

Table 45: Server Information Fields

| Field | Description |
|---|---|
| **Name** | The name of the server Lumension EMSS is installed on. |
| **URL** | The URL of the server Lumension EMSS is installed on. |
| **Serial Number** | The serial number used by Lumension EMSS. |
| **Operating System** | The operating system installed and running on the Lumension EMSS Server. |
| **Operating System Service Pack** | The service pack applied to the operating system, if applicable. |
| **Operating System Version** | The operating system version number. |
| **Installation Date** | The date and time Lumension EMSS was installed. |
| **Last Connected** | The date and time Lumension EMSS last connected to the Global Subscription Server (GSS). |
| **Subscription Service ID** | The ID assigned to Lumension EMSS upon registration with the GSS. |
| **Replication Service Version** | The replication service version number. |
| **Last Agent Connection** | The date and time a registered Lumension EMSS Agent last connected to the Lumension EMSS Server. |
| **Total Agents Registered** | The total number of agents registered with Lumension EMSS. |
| **Storage Volume Free Space** | The amount of free disk space on your storage volume. |
| **System Root Free Space** | The amount of free disk space on your system volume. |
| **IIS Version** | The Internet Information Services (IIS) version installed. |
| **.NET Version** | The .NET Framework version(s) installed. |
| **MDAC Version** | The Microsoft Data Access Components (MDAC) version. The **Detail** button adjacent to the field opens the ***MDAC File Version Information*** dialog. |
| **SQL File Version** | The SQL Server file version installed. |
| **SQL Version** | The SQL Server version number followed by detailed information. |

## Viewing the MDAC File Version Information Dialog

Navigate to this dialog to view MDAC file version information.

You can access this dialog from the ***Technical Support*** page.

1. Select **Help** > **Technical Support**.
2. Click **Detail...**.

   **Step Result:** The ***MDAC File Version Information*** dialog opens.

3. View the MDAC file version data.

## MDAC File Version Information

The ***MDAC File Version Information*** dialog lists the individual `.dll` files included within the version of Microsoft Data Access Components (MDAC) installed on your Lumension Endpoint Management and Security Suite server. To open this dialog, click the **Detail** button within **Component Version Information**.

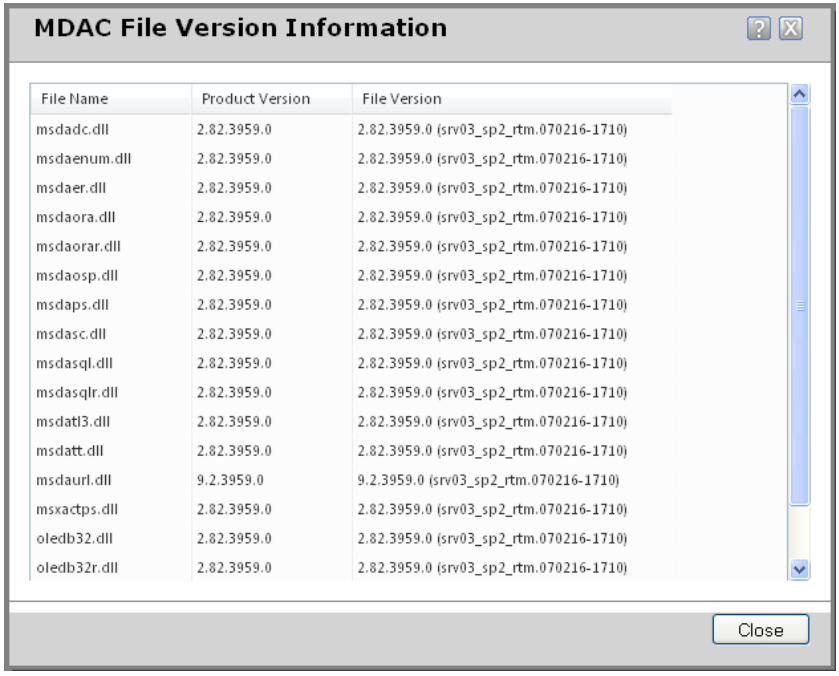



Figure 33: MDAC File Version Information Dialog

The following table describes the contents of the ***MDAC File Version Information*** dialog.

Table 46: MDAC File Version Information

| Column | Description |
|---|---|
| **File Name** | The name of the MDAC `.dll` file. |
| **Product Version** | The product version number of the file. |

| Column | Description |
|---|---|
| **File Version** | The file version number of the file. |

## Suite Version Information

**Suite Version Information** displays the version number of Lumension Endpoint Management and Security Suite (Lumension EMSS), each platform component installed, and each module component installed.

The following table describes each **Suite Version Information** field.

Table 47: Suite Version Information Fields

| Field | Description |
|---|---|
| **Server Suite Version** | The version number of Lumension EMSS installed on your Lumension EMSS server. |
| **Core Version** | The version number of the Lumension EMSS core installed on your Lumension EMSS server. |
| ***Module* Version** | The name and version number of a Lumension EMSS module installed on your Lumension EMSS server. A field appears for each module installed on your server. |

## Regenerating OS Packs

This task regenerates and synchronizes the relevant information for each of the operating systems supported by Lumension Endpoint Management and Security Suite.

Regenerate OS packs from the ***Technical Support*** page.

1. Select **Help** > **Technical Support**.

   **Step Result:** The ***Technical Support*** page opens.

2. Click **Regenerate OS Packs**.

   **Step Result:** A dialog displays, asking you to acknowledge the regeneration.

3. Click **OK**.

   **Step Result:** A dialog displays, asking you to acknowledge that the regeneration has been scheduled.

4. Acknowledge the scheduling by clicking **OK**.

**Result:** The OS pack regeneration is scheduled. The regeneration occurs the next time the Lumension Endpoint Management and Security Suite server communicates with the Global Subscription Server.

## Exporting Technical Support Data

You can export the data listed on the ***Technical Support*** page for reporting and analytical purposes.

Exported data includes **Technical Support Options**, **Server Information**, and **Suite Version Information**. To export this data, select **Help** > **Technical Support** and click **Export**. For additional information, refer to *Exporting Data* on page 37.

# The Product Licensing Page

Use this page to view, validate, and export license information. It summarizes product component licenses applicable to your endpoint management activities. Product information is updated during daily replication with the Global Subscription Server. Additionally, the page lists how many agent licenses you have, how many of those licenses are in use, and how many of those licenses are available.

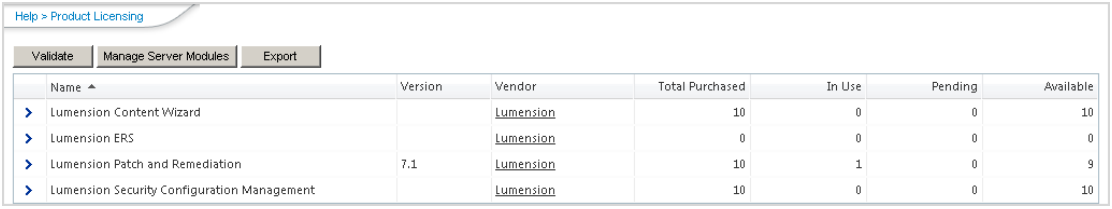



Figure 34: Product Licensing Page

## Viewing the Product Licensing Page

Navigate to this page to view information about license validity and daily replication.

You can access this page at any time through the navigation menu.

1. Select **Help** > **Product Licensing**.
2. View your product license data.

## The Product Licensing Page Buttons

Use these buttons to initiate functions related to licensing information.

The following table describes each button.

Table 48: Product Licensing Page Buttons

| Button | Function |
|---|---|
| **Validate** | Initiates a license replication that searches for any changes to your license data. For additional information, refer to *Initiating Subscription License Replication Jobs* on page 93.<br>**Note:** This field does not definitively indicate that replication is working. |
| **Launch Installation Manager...** | Opens Lumension Installation Manager in a new browser window to the ***New/ Updated Components*** tab. For additional information on usingLumension Installation Manager, refer to *Lumension Endpoint Management and Security Suite 7.1 User Guide* (*http://portal.lumension.com*). |

| Button | Function |
|---|---|
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br><br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |

## The Product Licensing Page List

This list itemizes licensing information for each Lumension Endpoint Management and Security Suite module. View this table for an overview of license availability.

The following reference describes the list columns.

Table 49: Product Licensing Page List

| Column | Description |
|---|---|
| **Name** | The product module name. |
| **Version** | The product module version number. |
| **Vendor** | The source of the license. The vendor name is a link to the vendor home page, which opens in a new window. |
| **Total Purchased** | The total number of licenses purchased for the module. |
| **In Use** | The number of licenses in use for the module. |
| **Pending** | The number of licenses pending use or removal for the module. |
| **Available** | The number of licenses available for the module. |

The list item for each product module can be expanded to display license group information. License groups are blocks of licenses purchased at a time. For example, you may have 3 license groups comprising 500 total licenses. Initially, a group of 300 licenses was purchased, and then 2 additional groups of 100 licenses were added during subsequent quarters.

To expand a list item, click the **rotating chevron** (>). The following table describes each column that displays after expanding a list item.

Table 50: Expanded Product Licensing List Item

| Column | Description |
|---|---|
| **Purchase Date (Server)** | The date and time the license group was purchased. |
| **Effective Date (Server)** | The date and time the license went into effect. This date is the first day that the licenses became valid, not necessarily the installation date. |

| Column | Description |
|---|---|
| **Expiration Date (Server)** | The date and time the license group expires. |
| **Purchased** | The total number of licenses purchased in the license group. |

## Initiating Subscription License Replication Jobs

Initiate these jobs to validate license replication. This replication searches for any changes to your license data.

Validate product licensing from the ***Product Licensing*** page.

1. Select **Help** > **Product Licensing**.

   **Step Result:** The ***Product Licensing*** page opens.

2. Click **Validate**.

   **Step Result:** A dialog opens, asking you to acknowledge the validation initiation.

3. Click **OK**.

**Result:** The job begins. Completion may take several minutes.

## Exporting Product Information

You can export product information data to a comma separated value (.csv) file for reporting and analytical purposes.

To export this data, select **Help** > **Product Licensing** and click **Export**. For additional information, refer to *Exporting Data* on page 37.

# Chapter 5

# Discovering Assets

**In this chapter:**


- About Discovery Scan Jobs
- The Discovery Scan Process
- Working with Discovery Scan Jobs
- About Agent Management Jobs
- Working with Agent Management Jobs


Use Lumension Endpoint Management and Security Suite (Lumension EMSS) to discover *assets*. Assets are endpoints, endpoint inventories (endpoint hardware and software), and other devices (printers, routers, and so on). By discovering assets, you can detect endpoints within your network and then remotely install agents on them.

Lumension EMSS discovers assets using *discovery scan jobs*.

After discovering endpoints, you can then install agents on them using *agent management jobs*, which are jobs that install agents on endpoints. Following agent installation, communication between agents and Lumension EMSS begins, leading to security management activity.

## About Discovery Scan Jobs

Lumension Endpoint Management and Security Suite uses network-based scanning to detect endpoints (computers, laptops, and so on) and devices (routers, printers, and so on) on your network. These scans are called *discovery scan jobs*.

The primary purpose of the discovery scan job is to detect endpoints that have no agents installed. After these unprotected endpoints are detected, you can install agents on them, ensuring your endpoints are safe from potential security breaches. The secondary purpose of the discovery scan job is to provide a census of network assets and other information. This census includes:

- Endpoints
- Endpoint software
- Endpoint hardware
- Endpoint address information
- Endpoint operating system information
- Devices (printers, routers, and so on)

Discovery scan jobs are fully customizable. When configuring a discovery scan jobs, you can control the following job behavior:

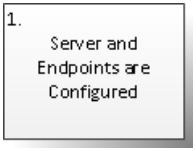
- Job date and time
- Job recurrence
- Job discovery methods used to define scan targets
- Job discovery options used to acquire asset information
- Job credentials used to acquire asset information

**Important:** Windows Vista, Windows Server 2008, and Windows 7 target endpoints must have both **Network discovery** and **File sharing** enabled. If target endpoints do not have these features enabled, they are not discovered during discovery scan jobs or agent management jobs. For additional information refer to *Configuring Post-Windows Vista Endpoints for Discovery* on page 331.

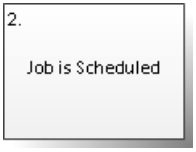
## The Discovery Scan Process

Discovery scan jobs locate endpoints in your network and scan them for endpoint information.

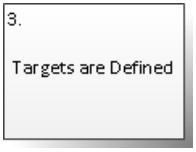
The following flowchart describes the sequence of events during the process of scanning for endpoints.



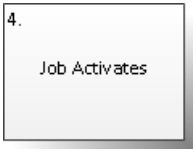

Configure your server and endpoints for scanning. To scan for endpoints, your Lumension Endpoint Management and Security Suite server and your network endpoints must be configured for scanning. For additional information, refer to *Configuring Post-Windows Vista Endpoints for Discovery* on page 331.



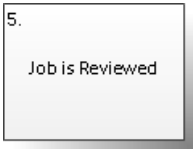

Schedule a scan job. You can schedule scan jobs to run immediately or at a defined day and time.




Define targets for scanning. During scanning, your scan job searches for the targets you define.




At the defined time, your discovery scan job activates, scanning for defined targets. Jobs active either immediately following job configuration or at a scheduled date and time.




When your job completes, you can review your scan job results from the ***Job Results*** page. Results include information about the endpoints scanned.

# Working with Discovery Scan Jobs

There are several tasks associated with the discovery of network assets. These tasks are available from the navigation menu under **Discover**.


- *Discovering Assets by Discovery Scan Job* on page 97
- *Editing Targets* on page 107


## Discovering Assets by Discovery Scan Job

Discovery scan jobs find endpoints and devices in your network. Use these jobs to schedule future jobs, reoccurring jobs, or jobs that only use certain discovery options.

You can create a discovery scan job from the navigation menu or by clicking a toolbar button on the ***Job Results*** page.

**Important:** Windows Vista, Windows Server 2008, and Windows 7 target endpoints must have both **Network discovery** and **File sharing** enabled. If target endpoints do not have these features enabled, they are not discovered during discovery scan jobs or agent management jobs. For additional information refer to *Configuring Post-Windows Vista Endpoints for Discovery* on page 331.

1. Select **Discover** > **Assets**.

   **Step Result:** The ***Discover Assets Wizard*** opens to the ***Job Name and Scheduling*** page.

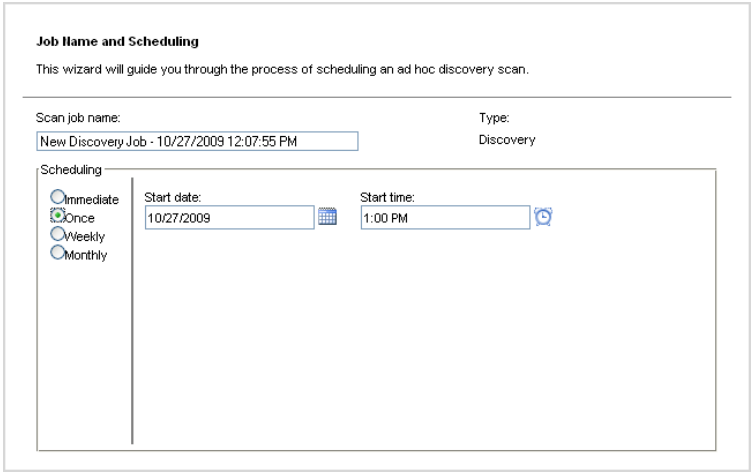



Figure 35: Job Name and Scheduling Page

2. If desired, type a new name in the **Scan job name** field.

   **Note:** By default, new discovery scan jobs are named `New Discovery Job`, followed by the server date and time, which is formatted according to your server's *ClientAdmin* user locale setting.

3. Schedule the job.

   Use one of the following methods.

| Method | Steps |
|---|---|
| **To schedule an immediate job:** | Select the **Immediate** option. |
| **To schedule a one-time job:** | 1. Ensure the **Once** option is selected.<br>2. Define a start date. Complete one of the following sub step sets.<br>To define a start date manually:<br>**a.** Type the start date in the **Start date** field using a `mm/dd/yyyy` format.<br>To define a start date using a menu:<br>**a.** Click the **Calender** icon.<br>**b.** Select a date from the calender. If necessary, use the arrow icons to open change months.<br>3. Define a start time. Complete one of the following sub step sets.<br>To define a start time manually:<br>**a.** Type the start time in the **Start time** field using a `hh:mm` format followed by `AM` or `PM`. The **Start time** field supports both 12- and 24-hour time.<br>To define a start time using a list:<br>**a.** Click the **Clock** icon.<br>**b.** Select a time from the menu.<br>**Note:** Scheduling a one-time job for a past date and time will launch the job immediately. |

| Method | Steps |
| --- | --- |
| **To schedule a recurring weekly job:** | **1.** Select the **Weekly** option.<br>**2.** Define a start date. Complete one of the following sub step sets.<br>To define a start date manually:<br>**a.** Type the start date in the **Start date** field using a `mm/dd/yyyy` format.<br>To define a start date using a menu:<br>**a.** Click the **Calender** icon.<br>**b.** Select a date from the calender. If necessary, use the arrow icons to open change months.<br>**3.** Define a start time. Complete one of the following sub step sets.<br>To define a start time manually:<br>**a.** Type the start time in the **Start time** field using a `hh:mm` format followed by `AM` or `PM`. The **Start time** field supports both 12- and 24-hour time.<br>To define a start time using a list:<br>**a.** Click the **Clock** icon.<br>**b.** Select a time from the menu. |

| Method | Steps |
|---|---|
| **To schedule a recurring monthly job:** | **1.** Select the **Monthly** option.<br>**2.** Define a start date. Complete one of the following sub step sets.<br>To define a start date manually:<br>**a.** Type the start date in the **Start date** field using a `mm/dd/yyyy` format.<br>To define a start date using a menu:<br>**a.** Click the **Calender** icon.<br>**b.** Select a date from the calender. If necessary, use the arrow icons to open change months.<br>**3.** Define a start time. Complete one of the following sub step sets.<br>To define a start time manually:<br>**a.** Type the start time in the **Start time** field using a `hh:mm` format followed by `AM` or `PM`. The **Start time** field supports both 12- and 24-hour time.<br>To define a start time using a list:<br>**a.** Click the **Clock** icon.<br>**b.** Select a time from the menu. |

**Note:** One-time and recurring jobs scheduled for the last day of a 31-day month are automatically rescheduled for the last day of shorter months.

4. Click **Next**.

   **Step Result:** The ***Targets*** page opens.

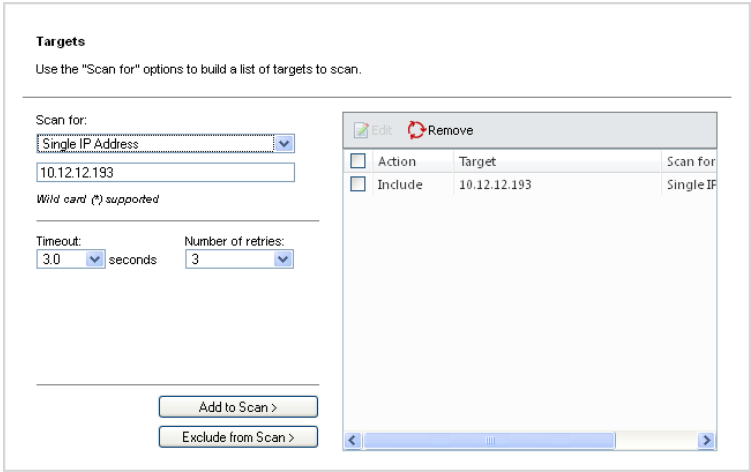



Figure 36: Targets Page

5. If necessary, define targets (endpoints) for the job to locate.

   Use one or more of the following discovery methods.

| Method | Steps |
|---|---|
| **To define targets using a single IP address:** | 1. From the **Scan for** list, select **Single IP Address**.<br>2. Type an IP address in the empty field. Wildcards are supported. For additional information, refer to *Defining Targets Using Wildcards* on page 308.<br>3. If necessary, edit the **Timeout** list. The **Timeout** list defines the number of seconds before a scan fails due to inactivity for a particular target. Under most network conditions, the **Timeout** field does not require editing.<br>4. If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a scan retries on that target if the scan times out. |

| Method | Steps |
|---|---|
| **To define targets using an IP range:** | 1. From the **Scan for** list, select **IP Range**.<br>2. In the first empty field, type the beginning of IP range. Wildcards are supported. For additional information, refer to *Defining Targets Using Wildcards* on page 308.<br>3. In the second empty field, type the ending of the IP range.<br>4. If necessary, edit the **Timeout** list. The **Timeout** list defines the number of seconds before a scan fails due to inactivity for that particular target. Under most network conditions, the **Timeout** field does not require editing.<br>5. If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a scan retries on that target if the scan times out. |
| **To define targets using a computer name:** | 1. From the **Scan for** list, select **Computer name**.<br>2. In the empty field, type an endpoint name in one of the following formats: `endpointname` or `domain\endpointname`. |
| **To define targets using network neighborhood:** | 1. From the **Scan for** list, select **Network Neighborhood**.<br>2. From the second list, select the desired network neighborhood. |
| **To define targets using active directory:** | 1. From the **Scan for** list, select **Active Directory**.<br>2. In the **Fully-qualified domain name** field, type the DNS domain name of the domain controller you want to scan. For example, if your domain controller DNS name is *box.domain.company.local*, you would type *domain.company.local* in this field.<br>3. In the **Organizational Unit** field, type the active directory organizational unit string from specific to broad (optional). The omission of this field returns job results containing the full contents of *all* the active directory organizational units.<br>4. In the **Domain controller** field, type the domain controller IP address.<br>5. In the **Username** field, type a user name that authenticates with the domain controller. Type the user name in one of the following format: `domainname\username` or `username`.<br>6. In the **Password** field, type the password associated with the user name. |

| Method | Steps |
|---|---|
| **To define targets using an imported file:** | 1. From the **Scan for** list, select **Import file**.<br>2. Click **Browse**.<br>3. Browse to the file you want to use for target discovery. The following file types are supported: `.txt` and `.csv`.<br>4. Click **Open**. |

6. Add targets to the wizard list. This list indicates whether defined targets are included in or excluded from the job.

   Use one of the following methods.

| Method | Steps |
|---|---|
| **To include defined targets in the job:** | Click **Add to Scan**. |
| **To exclude defined targets from the job:** | Click **Exclude from Scan**. |

**Note:** You must include at least one target for **Next** to become available. You can also delete targets from the list by selecting the applicable check boxes and clicking **Remove**.

7. If desired, define additional targets and add them to the list.
8. Click **Next**.

   **Step Result:** The ***Scan Options*** page opens.

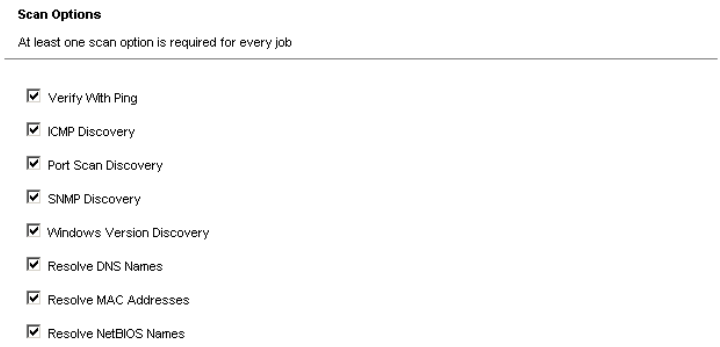



Figure 37: Scan Options

9. Select or clear the desired **Scan Options**.
   The following table defines each **Scan Option**.

| Option | Description |
|---|---|
| **Verify With Ping** | Jobs using this option send ping requests to all network endpoints targeted for discovery. Endpoints that respond to the request are flagged for scanning; unresponsive endpoints are skipped. Endpoints unresponsive to **Verify With Ping** are not scanned by other selected discovery options.<br>**Note:** Anti-virus software and host firewalls may block **Verify With Ping**. If necessary, adjust antivirus and firewall configurations to permit ping requests. |
| **ICMP Discovery** | Jobs using this option request a series of echoes, information, and address masks from endpoints. Endpoint responses are then compared to a list of known ICMP fingerprints to identify endpoint operating systems.<br>**Note:** **ICMP Discovery** is ineffective on endpoints configured to ignore ICMP requests. For best results identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**. |
| **Port Scan Discovery** | Jobs using this option perform a limited scan on endpoint FTP, Telnet, SSH, SMTP, and HTTP ports. Based on the application banners found in these ports, endpoint operating systems are generically identified.<br>**Note:** For best results in identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**. |
| **SNMP Discovery** | Jobs using this option request system properties for SNMP devices (routers, printers, and so on) from the management information base. Following credential authentication, SNMP devices are identified.<br>**Note:** Without authenticated credentials, SNMP devices ignore **SNMP Discovery** requests. In this event, one of two outcomes occur: the SNMP device is misidentified as a UNIX endpoint or the SNMP device is not detected. Jobs with no SNMP credentials use the *public* credential by default. |

| Option | Description |
|---|---|
| **Windows Version Discovery** | Jobs using this option identify an endpoint's specific version of Windows following generic operating system identification during **ICMP** or **Port Scan Discovery**.<br><br>**Note:** Correct operating system identification is contingent upon authenticated credentials. This option must be used in conjunction with either **ICMP** or **Port Scan Discovery**. |
| **Resolve DNS Names** | Jobs using this option acquire the endpoint DNS name through a local DNS server query. These names are displayed in job results for easy endpoint identification. |
| **Resolve MAC Addresses** | Jobs using this option acquire endpoint MAC addresses through endpoint queries. These addresses are displayed in job results for easy endpoint identification.<br><br>**Note:** Monitor network inventory reports to prevent MAC address spoofing that may alter the **Resolve MAC Addresses** results. |
| **Resolve NetBIOS Names** | Jobs using this option acquire endpoint NetBIOS names through WINS NetBIOS mapping. These names are displayed in job results for easy endpoint identification.<br><br>**Note:** Security-hardened networks running Windows 2000, Windows 2003, or Windows XP may require enabling of NetBIOS over TCP/IP for **Resolve NetBIOS Names** to acquire NetBIOS names. Additionally, firewalls protecting endpoints using Windows XP Professional SP2 may require adjustment to permit NetBIOS communication. |

**10.** Click **Next**.

**Step Result:** The ***Credentials*** page opens.

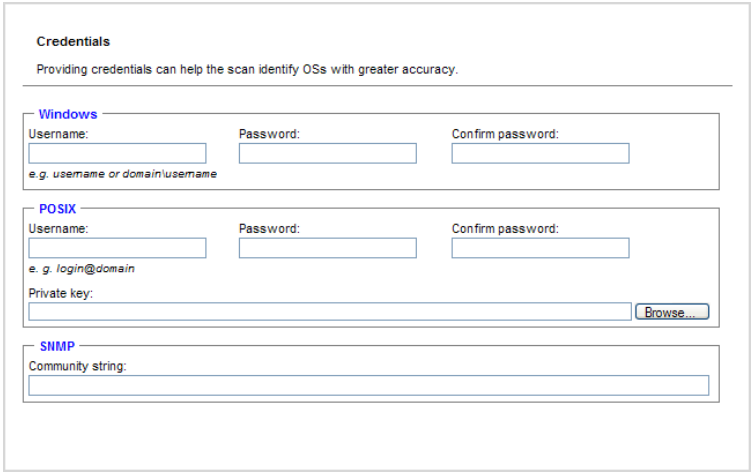



Figure 38: Credentials Page

**11.** If necessary, define **Windows** credentials.

Type the applicable information in the following fields.

**Note:** When configuring an agent management job, you must define valid Windows credentials.

| Field | Description |
|---|---|
| **Username** | A user name that authenticates with Windows endpoints. Type the user name in a local format (`username`) or a domain format (`domain/username`). |
| **Password** | The password associated with the **Username**. |
| **Confirm password** | The **Password** retyped. |

**12.** If desired, select the **Validate credentials access level** check box.

Selecting this check box validates the access levels that the entered credentials achieve on scan targets. This information is useful when determining if credentials provided the access necessary for agent management jobs.

**Note:** Selecting this option could increase job run time.

13. If necessary, define **POSIX** credentials (credentials for UNIX-based operating systems).
    Type the applicable information in the following fields.

| Field | Description |
|---|---|
| **Username** | A user name that authenticates with POSIX endpoints. Type the user name in the following format: `login@domain`. |
| **Password** | The password associated with the **Username**. |
| **Confirm password** | The **Password** retyped. |

14. If necessary, define a **POSIX** private key.
    a) Click **Browse**.
    b) Browse to the applicable `.txt` file.
    c) Click **Open**.
15. If necessary, define an **SNMP** community string that authenticates with network devices.
    a) Type the applicable community string in the **Community string** field.
16. Click **Finish**.

**Result:** The ***Discover Assets Wizard*** closes. Depending on how you scheduled the job, the discover assets job moves to either the ***Job Results*** page's ***Scheduled*** or ***Active*** tab.

## Editing Targets

While configuring jobs, you can edit items included in the **Targets** list.

Edit **Target** list items from the ***Targets*** page.

1. From the **Targets** list, select the check box associated with the item you want to edit.
2. Click **Edit**.

**Step Result:** The ***Edit Targets*** dialog opens.

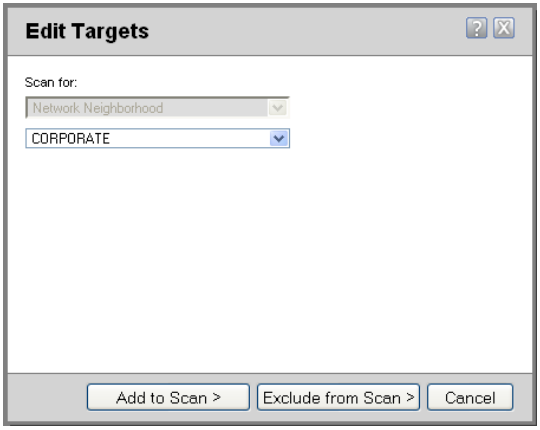



Figure 39: Edit Targets Dialog

3. Based on the type of discovery method, edit the item.

| Discovery Method | Steps |
|---|---|
| **Single IP Address** | 1. Type a new IP address in the field. Wildcards are supported. For additional information, refer to *Defining Targets Within an Imported File* on page 309.<br>2. If necessary, edit the **Timeout** list. The **Timeout** list defines the number of seconds before a scan fails due to inactivity. Under most network conditions, the **Timeout** field does not require editing.<br>3. If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a discover assets scan retries if the scan times out. |
| **IP Range** | 1. In the field, type the beginning of IP range. Wildcards are supported. For additional information, refer to *Defining Targets Within an Imported File* on page 309.<br>2. In the field, type the ending of the IP range.<br>3. If necessary, edit the **Timeout** list. The **Timeout** list defines the number of seconds before a scan fails due to inactivity. Under most network conditions, the **Timeout** field does not require editing.<br>4. If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a discover assets scan retries if the scan times out. |
| **Computer Name** | In the empty field, type a new endpoint name in one of the following formats: `endpointname` or `domain\endpointname`. |
| **Network Neighborhood** | From list, select the desired network neighborhood. |

| Discovery Method | Steps |
|---|---|
| **Active Directory** | 1. In the **Fully-qualified domain name** field, type the DNS domain name of the domain controller you want to scan. For example, if your domain controller's DNS name was *box.domain.company.local*, you would type *domain.company.local* in this field.<br>2. In the **Organizational Unit** field, type the active directory's organizational unit string from specific to broad (optional). The omission of this field returns job results containing the full contents of *all* the active directory's organizational units.<br>3. In the **Domain controller** field, type the domain controller's IP address.<br>4. In the **Username** field, type user name that will authenticate with the domain controller. Type the user name in one of the following format: `domainname\username` or `username`.<br>5. In the **Password** field, type the password associated with the user name. |

4. Include or exclude the target(s) from the scan.
   - To include the target(s), click **Include Targets**.
   - To exclude the target(s), click **Exclude Targets**.

**Result:** The **Targets** list reflects your changes.

## About Agent Management Jobs

*Agent Management jobs* let you install Lumension Endpoint Management and Security Suite agents remotely on multiple endpoints within your network. Use of agent management jobs eases the burden on network administrators.

These jobs are configured in the agent management job wizard, which is similar in appearance to the discovery scan job wizard.

The initial portion of an agent management job is identical to a discovery scan job; it detects endpoints and their operating systems in your network via pinging and endpoint scanning.

Agent management jobs then begin their next function: agent installation. Based on the operating system information found during scanning, agent management jobs determine which type of agent to install on applicable endpoints. To access the endpoint, the agent management job provides the endpoint with applicable credentials. These credentials are entered during job configuration. After the endpoint authenticates the offered

credentials, the agent management job begins agent installation. Installation occurs silently in an endpoint's background; endpoint users are unaware of the installation.

**Note:** Remember the following information when working with agent management jobs:

- Verify that the endpoints you are installing agents on are Windows-based. Unix-based endpoints are not agent management job-compatible.
- Gather the credentials for endpoints you are installing agents on. Successful job outcome is contingent upon authenticated credentials.
- Enable **Network discovery** and **File sharing** on Windows Vista, Windows Server 2008, and Windows 7 endpoints. These features must be enabled for targets to be discovered. For additional information, refer to *Configuring Post-Windows Vista Endpoints for Discovery* on page 331.
- Configure your server to allow agent management. For additional information, refer to *Configuring the Scanning System* on page 323.
- Configure your targets to allow agent management. For additional information, refer to *Configuring Endpoints for Agent Management Jobs (Pre-Windows Vista)* on page 326 or *Configuring Endpoints for Agent Management Jobs (Post-Windows Vista)* on page 334.

Following configuration of an agent management job, you can view it on the ***Job Results*** page. Based on how you scheduled the job, it appears on either the ***Scheduled*** tab or the ***Active*** tab. After the job finishes scanning and agent management, it moves to the ***Completed*** tab.

## Working with Agent Management Jobs

There are several tasks associated with agent installation on network endpoints. These tasks are available from the navigation menu under **Discover**.

- *Installing Agents by Agent Management Job* on page 111
- *Uninstalling Agents by Agent Management Job* on page 124

## Installing Agents by Agent Management Job

You can install agents upon network endpoints remotely by using agent management jobs. Installing agents remotely substantially eases an administrator's workload, since they do not have to install agents locally.

**Prerequisites:**

- Verify that the endpoints you are installing agents on are Windows-based. Unix-based endpoints are not agent management job-compatible.
- Gather the credentials for endpoints you are installing agents on. Successful job outcome is contingent upon authenticated credentials.
- Enable **Network discovery** and **File sharing** on Windows Vista, Windows Server 2008, and Windows 7 endpoints. These features must be enabled for targets to be discovered. For additional information, refer to *Configuring Post-Windows Vista Endpoints for Discovery* on page 331.
- Configure your server to allow agent management. For additional information, refer to *Configuring the Scanning System* on page 323.
- Configure your targets to allow agent management. For additional information, refer to *Configuring Endpoints for Agent Management Jobs (Pre-Windows Vista)* on page 326 or *Configuring Endpoints for Agent Management Jobs (Post-Windows Vista)* on page 334.

Configuration of agent management jobs is similar to configuration of discovery scan jobs. Configuration occurs in the ***Install Agents Wizard***.

**Note:** Agent management jobs can only manage Windows-based endpoints. Unix-based endpoints are not agent management job-compatible.

1. Begin configuration of the ***Install Agent Wizard***.

   Complete one of the following substep sets to being configuration.

| Context | Steps |
|---|---|
| **To open the Wizard without targets predefined:** | Select **Discover** > **Assets and Install Agents...** |

| Context | Steps |
|---|---|
| **To open the Wizard with target predefined:** | 1. Select **Manage** > **Endpoints**.<br>2. Select the endpoints you want to install agents on.<br>3. From the toolbar, select **Manage Agents...** > **Install Agents...** |

**Step Result:** The wizard opens to the ***Job Name and Scheduling*** page.

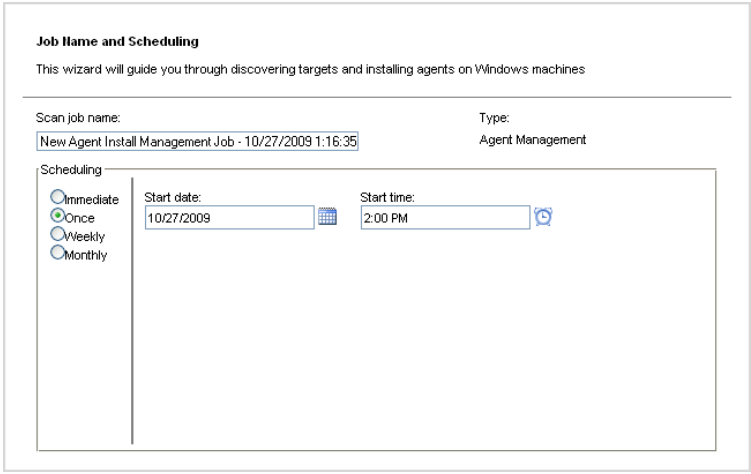



Figure 40: Job Name and Scheduling Page

2. If desired, type a new name in the **Scan job name** field.

**Note:** By default, new agent management jobs for installation are named `New Agent Install Management Job`, followed by the server's date and time.

3. Schedule the job.

   Use one of the following methods.

| Method | Steps |
|---|---|
| **To schedule an immediate job:** | Select the **Immediate** option. |

| Method | Steps |
|---|---|
| **To schedule a one-time job:** | **1.** Ensure the **Once** option is selected.<br>**2.** Define a start date. Complete one of the following sub step sets.<br>To define a start date manually:<br>**a.** Type the start date in the **Start date** field using a `mm/dd/yyyy` format.<br>To define a start date using a menu:<br>**a.** Click the **Calender** icon.<br>**b.** Select a date from the calender. If necessary, use the arrow icons to open change months.<br>**3.** Define a start time. Complete one of the following sub step sets.<br>To define a start time manually:<br>**a.** Type the start time in the **Start time** field using a `hh:mm` format followed by `AM` or `PM`. The **Start time** field supports both 12- and 24-hour time.<br>To define a start time using a list:<br>**a.** Click the **Clock** icon.<br>**b.** Select a time from the menu.<br>**Note:** Scheduling a one-time job for a past date and time will launch the job immediately. |

| Method | Steps |
| --- | --- |
| **To schedule a recurring weekly job:** | **1.** Select the **Weekly** option.<br>**2.** Define a start date. Complete one of the following sub step sets.<br>To define a start date manually:<br>**a.** Type the start date in the **Start date** field using a `mm/dd/yyyy` format.<br>To define a start date using a menu:<br>**a.** Click the **Calender** icon.<br>**b.** Select a date from the calender. If necessary, use the arrow icons to open change months.<br>**3.** Define a start time. Complete one of the following sub step sets.<br>To define a start time manually:<br>**a.** Type the start time in the **Start time** field using a `hh:mm` format followed by `AM` or `PM`. The **Start time** field supports both 12- and 24-hour time.<br>To define a start time using a list:<br>**a.** Click the **Clock** icon.<br>**b.** Select a time from the menu. |

| Method | Steps |
| --- | --- |
| **To schedule a recurring monthly job:** | **1.** Select the **Monthly** option.<br>**2.** Define a start date. Complete one of the following sub step sets.<br>To define a start date manually:<br>**a.** Type the start date in the **Start date** field using a `mm/dd/yyyy` format.<br>To define a start date using a menu:<br>**a.** Click the **Calender** icon.<br>**b.** Select a date from the calender. If necessary, use the arrow icons to open change months.<br>**3.** Define a start time. Complete one of the following sub step sets.<br>To define a start time manually:<br>**a.** Type the start time in the **Start time** field using a `hh:mm` format followed by `AM` or `PM`. The **Start time** field supports both 12- and 24-hour time.<br>To define a start time using a list:<br>**a.** Click the **Clock** icon.<br>**b.** Select a time from the menu. |

**Note:** One-time and recurring jobs scheduled for the last day of a 31-day month are automatically rescheduled for the last day of shorter months.

4. Click **Next**.

   **Step Result:** The ***Targets*** page opens.

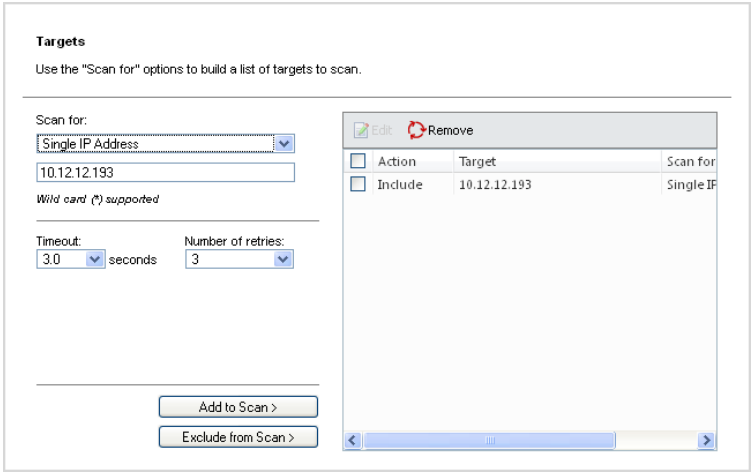



Figure 41: Targets Page

5. If necessary, define targets (endpoints) for the job to locate.

   Use one or more of the following discovery methods.

| Method | Steps |
|---|---|
| **To define targets using a single IP address:** | 1. From the **Scan for** list, select **Single IP Address**.<br>2. Type an IP address in the empty field. Wildcards are supported. For additional information, refer to *Defining Targets Using Wildcards* on page 308.<br>3. If necessary, edit the **Timeout** list. The **Timeout** list defines the number of seconds before a scan fails due to inactivity for a particular target. Under most network conditions, the **Timeout** field does not require editing.<br>4. If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a scan retries on that target if the scan times out. |

| Method | Steps |
|---|---|
| **To define targets using an IP range:** | 1. From the **Scan for** list, select **IP Range**.<br>2. In the first empty field, type the beginning of IP range. Wildcards are supported. For additional information, refer to *Defining Targets Using Wildcards* on page 308.<br>3. In the second empty field, type the ending of the IP range.<br>4. If necessary, edit the **Timeout** list. The **Timeout** list defines the number of seconds before a scan fails due to inactivity for that particular target. Under most network conditions, the **Timeout** field does not require editing.<br>5. If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a scan retries on that target if the scan times out. |
| **To define targets using a computer name:** | 1. From the **Scan for** list, select **Computer name**.<br>2. In the empty field, type an endpoint name in one of the following formats: `endpointname` or `domain\endpointname`. |
| **To define targets using network neighborhood:** | 1. From the **Scan for** list, select **Network Neighborhood**.<br>2. From the second list, select the desired network neighborhood. |
| **To define targets using active directory:** | 1. From the **Scan for** list, select **Active Directory**.<br>2. In the **Fully-qualified domain name** field, type the DNS domain name of the domain controller you want to scan. For example, if your domain controller DNS name is *box.domain.company.local*, you would type *domain.company.local* in this field.<br>3. In the **Organizational Unit** field, type the active directory organizational unit string from specific to broad (optional). The omission of this field returns job results containing the full contents of *all* the active directory organizational units.<br>4. In the **Domain controller** field, type the domain controller IP address.<br>5. In the **Username** field, type a user name that authenticates with the domain controller. Type the user name in one of the following format: `domainname\username` or `username`.<br>6. In the **Password** field, type the password associated with the user name. |

| Method | Steps |
|---|---|
| **To define targets using an imported file:** | 1. From the **Scan for** list, select **Import file**.<br>2. Click **Browse**.<br>3. Browse to the file you want to use for target discovery. The following file types are supported: `.txt` and `.csv`.<br>4. Click **Open**. |

6. Add targets to the wizard list. This list indicates whether defined targets are included in or excluded from the job.

   Use one of the following methods.

| Method | Steps |
|---|---|
| **To include defined targets in the job:** | Click **Add to Scan**. |
| **To exclude defined targets from the job:** | Click **Exclude from Scan**. |

**Note:** You must include at least one target for **Next** to become available. You can also delete targets from the list by selecting the applicable check boxes and clicking **Remove**.

7. If desired, define additional targets and add them to the list.

**Tip:** You can edit targets added to the list. For more information, see *Editing Targets* on page 107.

8. Click **Next**.

   **Step Result:** The ***Scan Options*** page opens.

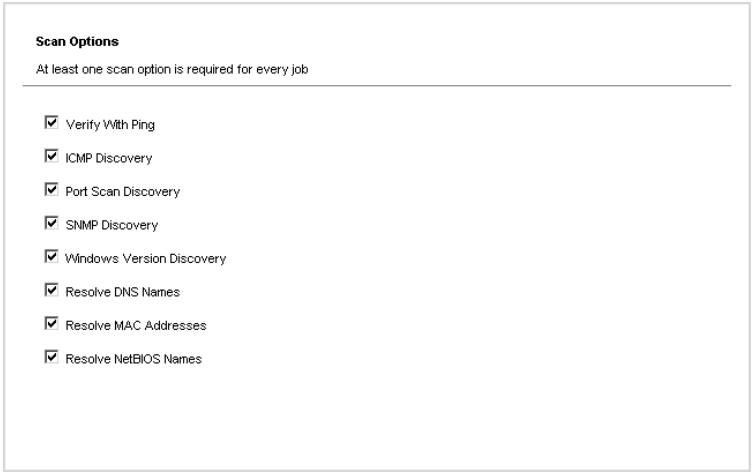



Figure 42: Scan Options Page

9. Select or clear the desired **Scan Options**.

   The following table defines each **Scan Option**.

| Option | Description |
|---|---|
| **Verify With Ping** | Jobs using this option send ping requests to all network endpoints targeted for discovery. Endpoints that respond to the request are flagged for scanning; unresponsive endpoints are skipped. Endpoints unresponsive to **Verify With Ping** are not scanned by other selected discovery options.<br>**Note:** Anti-virus software and host firewalls may block **Verify With Ping**. If necessary, adjust antivirus and firewall configurations to permit ping requests. |
| **ICMP Discovery** | Jobs using this option request a series of echoes, information, and address masks from endpoints. Endpoint responses are then compared to a list of known ICMP fingerprints to identify endpoint operating systems.<br>**Note:** **ICMP Discovery** is ineffective on endpoints configured to ignore ICMP requests. For best results identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**. |

| Option | Description |
|---|---|
| **Port Scan Discovery** | Jobs using this option perform a limited scan on endpoint FTP, Telnet, SSH, SMTP, and HTTP ports. Based on the application banners found in these ports, endpoint operating systems are generically identified.<br>**Note:** For best results in identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**. |
| **SNMP Discovery** | Jobs using this option request system properties for SNMP devices (routers, printers, and so on) from the management information base. Following credential authentication, SNMP devices are identified.<br>**Note:** Without authenticated credentials, SNMP devices ignore **SNMP Discovery** requests. In this event, one of two outcomes occur: the SNMP device is misidentified as a UNIX endpoint or the SNMP device is not detected. Jobs with no SNMP credentials use the *public* credential by default. |
| **Windows Version Discovery** | Jobs using this option identify an endpoint's specific version of Windows following generic operating system identification during **ICMP** or **Port Scan Discovery**.<br>**Note:** Correct operating system identification is contingent upon authenticated credentials. This option must be used in conjunction with either **ICMP** or **Port Scan Discovery**. |
| **Resolve DNS Names** | Jobs using this option acquire the endpoint DNS name through a local DNS server query. These names are displayed in job results for easy endpoint identification. |
| **Resolve MAC Addresses** | Jobs using this option acquire endpoint MAC addresses through endpoint queries. These addresses are displayed in job results for easy endpoint identification.<br>**Note:** Monitor network inventory reports to prevent MAC address spoofing that may alter the **Resolve MAC Addresses** results. |
| **Resolve NetBIOS Names** | Jobs using this option acquire endpoint NetBIOS names through WINS NetBIOS mapping. These names are displayed in job results for easy endpoint identification.<br>**Note:** Security-hardened networks running Windows 2000, Windows 2003, or Windows XP may require enabling of NetBIOS over TCP/IP for **Resolve NetBIOS Names** to acquire NetBIOS names. Additionally, firewalls protecting endpoints using Windows XP Professional SP2 may require adjustment to permit NetBIOS communication. |

**10.** Click **Next**.

**Step Result:** The ***Agent Options*** page opens.

**11.** Select the desired **Agent Options**.

These options control which version of the agent is installed on Windows-based endpoints.

a) Select an agent version from the **Agent version** list.

**Note:** The agent versions available for selection are defined by the **Agent Version Options**, which you can edit from the ***Options*** page ***Agents*** tab. For additional information, refer to *Agent Versions* on page 77.

b) Select the modules you want to install with the agent.

Select the check boxes associated with the modules you want to install.

c) If desired, select the **Overwrite existing agents** check box.

This option controls whether the agent management job skips targets that already have agents installed.

**Attention:** Selecting this option will cause data loss when an endpoint's Lumension Endpoint Management and Security Suite Agent is overwritten

Following initial agent installation, if the Patch and Remediation module is installed, the agent version will change if the applicable endpoint is subject to a conflicting agent version policy. Additionally, when installing the agent on Windows 2000 endpoints, the patch agent is installed (Patch and Remediation only).

**12.** Click **Next**.

**Step Result:** The ***Credentials*** page opens.

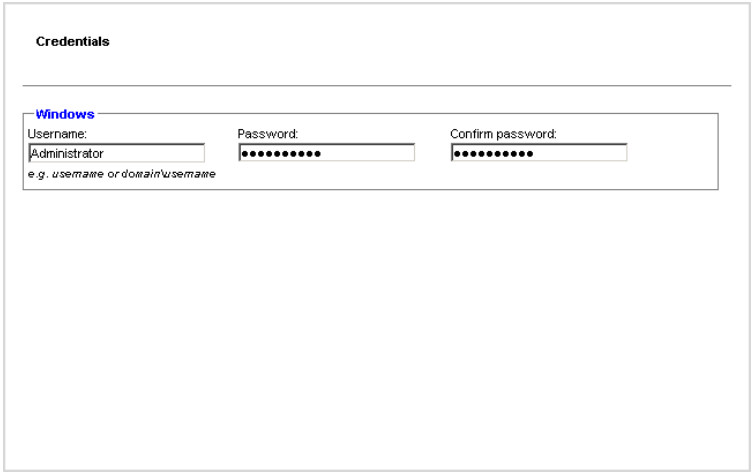



Figure 43: Credentials Page

**13.** Define **Windows** credentials for the target.

Type the applicable information in the following fields.

**Note:** When configuring an agent management job, you must define valid Windows credentials.

| Field | Description |
|---|---|
| **Username** | A user name that authenticates with Windows-based endpoints.<br>Type the user name in a local format (username) or a domain format (domain/username). |
| **Password** | The password associated with the **Username**. |
| **Confirm password** | The **Password** retyped. |

**14.** Click **Next**.

**Step Result:** The ***Agent Settings*** page opens.

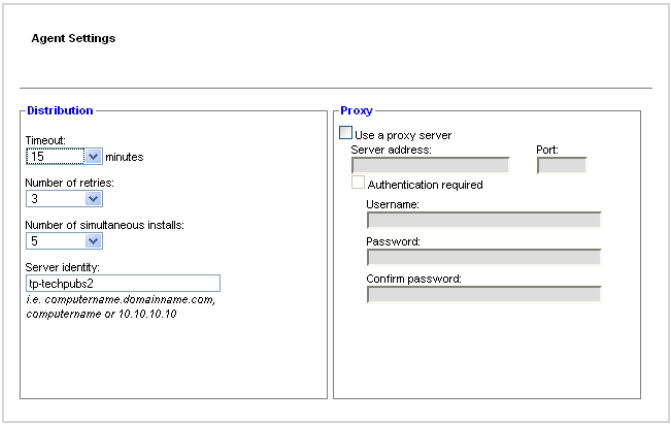



Figure 44: Agent Settings Page

**15.** Define the **Distribution** drop-down lists.

The following table describes each list their available values.

| List | Description |
|---|---|
| **Timeout** | Defines the number of minutes before the agent management job terminates due to a non-responsive agent installation or removal (0-30). |
| **Number of retries** | Defines the number of attempts an agent installation or removal will retry if the initial attempt fails (1-10). |

| List | Description |
|---|---|
| **Number of simultaneous installs** | Defines the maximum number of agents that can installed or removed simultaneously during the job (1-25). A value of `1` indicates that serial installs or removals should occur. |

16. Define how agents being installed name their Lumension Endpoint Management and Security Suite server within their registries by selecting a **Server Identity** option.

    The following table describes each option.

| Method | Steps |
|---|---|
| **To have agents reference the Lumension Endpoint Management and Security Suite server by its default name:** | Do not edit the **Server identity** field. The server will be identified on the agent according to the value set on the ***Agents*** tab on the ***Options*** page. For more information, see *Agent Installation* on page 75. |
| **To have agents reference the Lumension Endpoint Management and Security Suite server by a user-defined name:** | Type address information for your Lumension EMSS server in the **Server identity** field. Information must be entered in one of the following formats:<br>• `endpointname.domainname.com`<br>• `computername`<br>• `10.10.10.10`<br>**Note:** When using a name, it must be resolvable from the endpoint. |

17. Select a group from the **Custom Group** list.

    The **Custom Group** list determines which Lumension Endpoint Management and Security Suite group the agents are initially assigned to.

18. If using a proxy during agent management, select the **Use a proxy server** check box and define the following fields.

| Field | Description |
|---|---|
| **Server address** | The applicable proxy IP address. |
| **Port** | The applicable proxy port number used to communicate. |

19. If using a proxy during agent management, and that proxy requires authentication, select the **Authentication required** check box and define the following fields.

| Field | Description |
|---|---|
| **Username** | A user name that authenticates with the proxy. |

| Field | Description |
|---|---|
| **Password** | The password associated with the **Username**. |
| **Confirm password** | The **Password** retyped. |

**20.** Click **Finish**.

**Result:** The ***Schedule Agent Management Job - Install Wizard*** closes. Depending on how you configured the job, it moves to either the ***Scheduled*** tab or ***Active*** tab on the ***Job Results*** page. The job will run at the applicable time, installing agents on the defined targets, and move to ***Completed*** tab when finished.

**After Completing This Task:**

After the agent management job completes, install agent modules. For additional information, refer to *Managing Module Endpoint Components* on page 170.

## Uninstalling Agents by Agent Management Job

You can remotely uninstall agents from endpoints in your network using an agent management job. These jobs prevent administrators from having to uninstall agents locally.

**Prerequisites:**

- Verify that the endpoints you are installing agents on are Windows-based. Unix-based endpoints are not agent management job-compatible.
- Gather the credentials for endpoints you are installing agents on. Successful job outcome is contingent upon authenticated credentials.
- Enable **Network discovery** and **File sharing** on Windows Vista, Windows Server 2008, and Windows 7 endpoints. These features must be enabled for targets to be discovered. For additional information, refer to *Configuring Post-Windows Vista Endpoints for Discovery* on page 331.
- Configure your server to allow agent management. For additional information, refer to *Configuring the Scanning System* on page 323.
- Configure your targets to allow agent management. For additional information, refer to *Configuring Endpoints for Agent Management Jobs (Pre-Windows Vista)* on page 326 or *Configuring Endpoints for Agent Management Jobs (Post-Windows Vista)* on page 334.

Configuration of agent management is similar to a discover scan job. Configuration occurs in the ***Uninstall Agents Wizard***.

**1.** Begin configuration of the ***Uninstall Agent Wizard***.

Complete one of the follow substep sets to being configuration.

| Context | Steps |
|---|---|
| **To open the Wizard without targets predefined:** | Select **Discover** > **Assets and Uninstall Agents...** |

| Context | Steps |
|---|---|
| **To open the Wizard with target predefined:** | 1. Select **Manage** > **Endpoints**.<br>2. Select the endpoints you want to uninstall agents from.<br>3. From the toolbar, select **Manage Agents...** > **Uninstall Agents...** |

**Step Result:** The wizard opens to the ***Job Name and Scheduling*** page.

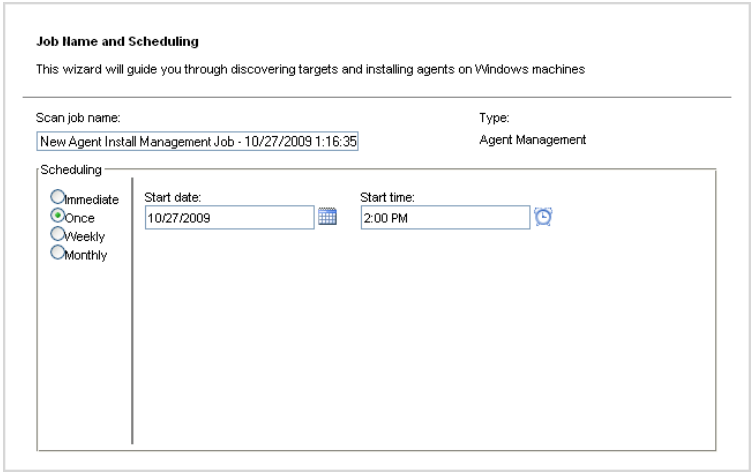



Figure 45: Job Name and Scheduling Page

2. If desired, type a new name in the **Scan job name** field.

**Note:** By default, new agent management jobs for uninstallation are named `New Agent Uninstall Management Job`, followed by the server date and time.

3. Schedule the job.

   Use one of the following methods.

| Method | Steps |
|---|---|
| **To schedule an immediate job:** | Select the **Immediate** option. |

| Method | Steps |
|---|---|
| **To schedule a one-time job:** | **1.** Ensure the **Once** option is selected.<br>**2.** Define a start date. Complete one of the following sub step sets.<br>To define a start date manually:<br>**a.** Type the start date in the **Start date** field using a `mm/dd/yyyy` format.<br>To define a start date using a menu:<br>**a.** Click the **Calender** icon.<br>**b.** Select a date from the calender. If necessary, use the arrow icons to open change months.<br>**3.** Define a start time. Complete one of the following sub step sets.<br>To define a start time manually:<br>**a.** Type the start time in the **Start time** field using a `hh:mm` format followed by `AM` or `PM`. The **Start time** field supports both 12- and 24-hour time.<br>To define a start time using a list:<br>**a.** Click the **Clock** icon.<br>**b.** Select a time from the menu.<br>**Note:** Scheduling a one-time job for a past date and time will launch the job immediately. |

| Method | Steps |
| --- | --- |
| **To schedule a recurring weekly job:** | **1.** Select the **Weekly** option.<br>**2.** Define a start date. Complete one of the following sub step sets.<br>To define a start date manually:<br>**a.** Type the start date in the **Start date** field using a `mm/dd/yyyy` format.<br>To define a start date using a menu:<br>**a.** Click the **Calender** icon.<br>**b.** Select a date from the calender. If necessary, use the arrow icons to open change months.<br>**3.** Define a start time. Complete one of the following sub step sets.<br>To define a start time manually:<br>**a.** Type the start time in the **Start time** field using a `hh:mm` format followed by `AM` or `PM`. The **Start time** field supports both 12- and 24-hour time.<br>To define a start time using a list:<br>**a.** Click the **Clock** icon.<br>**b.** Select a time from the menu. |

| Method | Steps |
|---|---|
| **To schedule a recurring monthly job:** | **1.** Select the **Monthly** option.<br>**2.** Define a start date. Complete one of the following sub step sets.<br>To define a start date manually:<br>**a.** Type the start date in the **Start date** field using a `mm/dd/yyyy` format.<br>To define a start date using a menu:<br>**a.** Click the **Calender** icon.<br>**b.** Select a date from the calender. If necessary, use the arrow icons to open change months.<br>**3.** Define a start time. Complete one of the following sub step sets.<br>To define a start time manually:<br>**a.** Type the start time in the **Start time** field using a `hh:mm` format followed by `AM` or `PM`. The **Start time** field supports both 12- and 24-hour time.<br>To define a start time using a list:<br>**a.** Click the **Clock** icon.<br>**b.** Select a time from the menu. |

**Note:** One-time and recurring jobs scheduled for the last day of a 31-day month are automatically rescheduled for the last day of shorter months.

4. Click **Next**.

   **Step Result:** The ***Targets*** page opens.

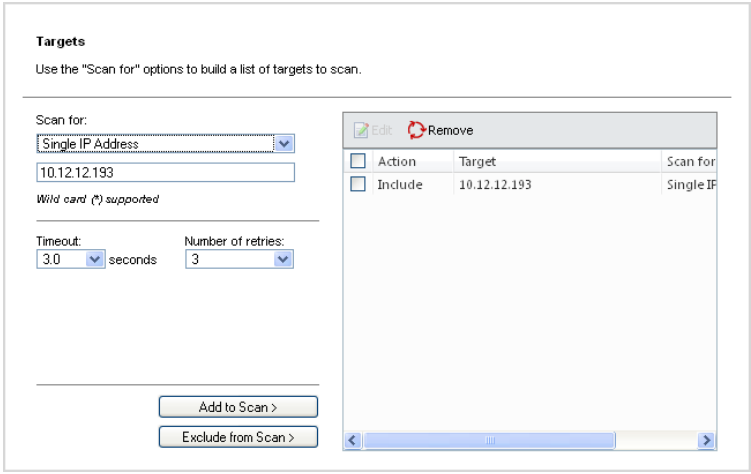



Figure 46: Targets Page

5. If necessary, define targets (endpoints) for the job to locate.

   Use one or more of the following discovery methods.

| Method | Steps |
|---|---|
| **To define targets using a single IP address:** | 1. From the **Scan for** list, select **Single IP Address**.<br>2. Type an IP address in the empty field. Wildcards are supported. For additional information, refer to *Defining Targets Using Wildcards* on page 308.<br>3. If necessary, edit the **Timeout** list. The **Timeout** list defines the number of seconds before a scan fails due to inactivity for a particular target. Under most network conditions, the **Timeout** field does not require editing.<br>4. If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a scan retries on that target if the scan times out. |

| Method | Steps |
|---|---|
| **To define targets using an IP range:** | 1. From the **Scan for** list, select **IP Range**.<br>2. In the first empty field, type the beginning of IP range. Wildcards are supported. For additional information, refer to *Defining Targets Using Wildcards* on page 308.<br>3. In the second empty field, type the ending of the IP range.<br>4. If necessary, edit the **Timeout** list. The **Timeout** list defines the number of seconds before a scan fails due to inactivity for that particular target. Under most network conditions, the **Timeout** field does not require editing.<br>5. If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a scan retries on that target if the scan times out. |
| **To define targets using a computer name:** | 1. From the **Scan for** list, select **Computer name**.<br>2. In the empty field, type an endpoint name in one of the following formats: `endpointname` or `domain\endpointname`. |
| **To define targets using network neighborhood:** | 1. From the **Scan for** list, select **Network Neighborhood**.<br>2. From the second list, select the desired network neighborhood. |
| **To define targets using active directory:** | 1. From the **Scan for** list, select **Active Directory**.<br>2. In the **Fully-qualified domain name** field, type the DNS domain name of the domain controller you want to scan. For example, if your domain controller DNS name is *box.domain.company.local*, you would type *domain.company.local* in this field.<br>3. In the **Organizational Unit** field, type the active directory organizational unit string from specific to broad (optional). The omission of this field returns job results containing the full contents of *all* the active directory organizational units.<br>4. In the **Domain controller** field, type the domain controller IP address.<br>5. In the **Username** field, type a user name that authenticates with the domain controller. Type the user name in one of the following format: `domainname\username` or `username`.<br>6. In the **Password** field, type the password associated with the user name. |

| Method | Steps |
|---|---|
| **To define targets using an imported file:** | 1. From the **Scan for** list, select **Import file**.<br>2. Click **Browse**.<br>3. Browse to the file you want to use for target discovery. The following file types are supported: `.txt` and `.csv`.<br>4. Click **Open**. |

6. Add targets to the wizard list. This list indicates whether defined targets are included in or excluded from the job.

   Use one of the following methods.

| Method | Steps |
|---|---|
| **To include defined targets in the job:** | Click **Add to Scan**. |
| **To exclude defined targets from the job:** | Click **Exclude from Scan**. |

**Note:** You must include at least one target for **Next** to become available. You can also delete targets from the list by selecting the applicable check boxes and clicking **Remove**.

7. If desired, define additional targets and add them to the list. For more information, see *Editing Targets* on page 107.
8. Click **Next**.

   **Step Result:** The ***Options*** page opens.

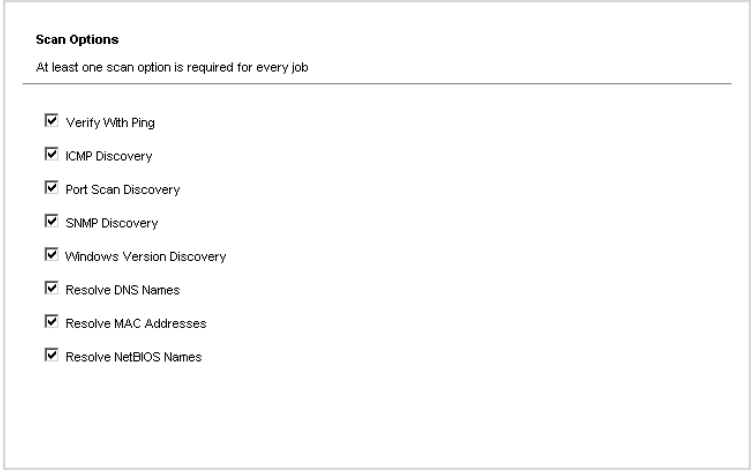



Figure 47: Options Page

9. Select or clear the desired **Scan Options**.
   The following table defines each **Scan Option**.

| Option | Description |
|---|---|
| **Verify With Ping** | Jobs using this option send ping requests to all network endpoints targeted for discovery. Endpoints that respond to the request are flagged for scanning; unresponsive endpoints are skipped. Endpoints unresponsive to **Verify With Ping** are not scanned by other selected discovery options.<br>**Note:** Anti-virus software and host firewalls may block **Verify With Ping**. If necessary, adjust antivirus and firewall configurations to permit ping requests. |
| **ICMP Discovery** | Jobs using this option request a series of echoes, information, and address masks from endpoints. Endpoint responses are then compared to a list of known ICMP fingerprints to identify endpoint operating systems.<br>**Note:** **ICMP Discovery** is ineffective on endpoints configured to ignore ICMP requests. For best results identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**. |
| **Port Scan Discovery** | Jobs using this option perform a limited scan on endpoint FTP, Telnet, SSH, SMTP, and HTTP ports. Based on the application banners found in these ports, endpoint operating systems are generically identified.<br>**Note:** For best results in identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**. |
| **SNMP Discovery** | Jobs using this option request system properties for SNMP devices (routers, printers, and so on) from the management information base. Following credential authentication, SNMP devices are identified.<br>**Note:** Without authenticated credentials, SNMP devices ignore **SNMP Discovery** requests. In this event, one of two outcomes occur: the SNMP device is misidentified as a UNIX endpoint or the SNMP device is not detected. Jobs with no SNMP credentials use the *public* credential by default. |

| Option | Description |
|---|---|
| **Windows Version Discovery** | Jobs using this option identify an endpoint's specific version of Windows following generic operating system identification during **ICMP** or **Port Scan Discovery**.<br><br>**Note:** Correct operating system identification is contingent upon authenticated credentials. This option must be used in conjunction with either **ICMP** or **Port Scan Discovery**. |
| **Resolve DNS Names** | Jobs using this option acquire the endpoint DNS name through a local DNS server query. These names are displayed in job results for easy endpoint identification. |
| **Resolve MAC Addresses** | Jobs using this option acquire endpoint MAC addresses through endpoint queries. These addresses are displayed in job results for easy endpoint identification.<br><br>**Note:** Monitor network inventory reports to prevent MAC address spoofing that may alter the **Resolve MAC Addresses** results. |
| **Resolve NetBIOS Names** | Jobs using this option acquire endpoint NetBIOS names through WINS NetBIOS mapping. These names are displayed in job results for easy endpoint identification.<br><br>**Note:** Security-hardened networks running Windows 2000, Windows 2003, or Windows XP may require enabling of NetBIOS over TCP/IP for **Resolve NetBIOS Names** to acquire NetBIOS names. Additionally, firewalls protecting endpoints using Windows XP Professional SP2 may require adjustment to permit NetBIOS communication. |

**10.** Click **Next**.

**Step Result:** The ***Credentials*** page opens.

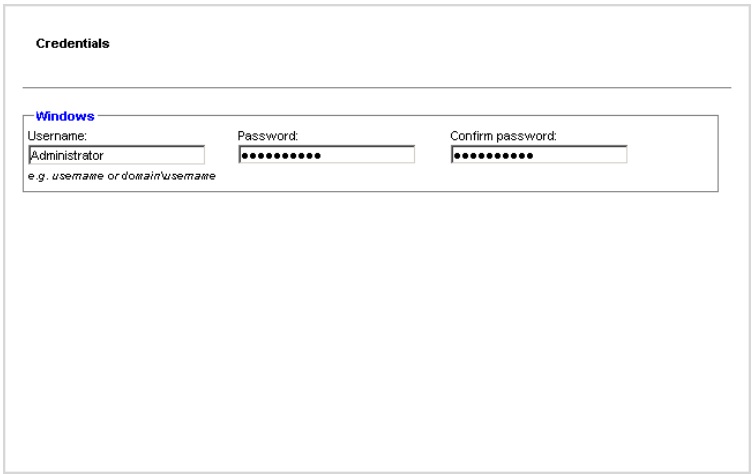



Figure 48: Credentials Page

**11.** Define **Windows** credentials for the target.

Type the applicable information in the following fields.

**Note:** When configuring an agent management job, you must define valid Windows credentials.

| Field | Description |
|---|---|
| **Username** | A user name that authenticates with Windows-based endpoints. Type the user name in a local format (username) or a domain format (domain/username). |
| **Password** | The password associated with the **Username**. |
| **Confirm password** | The **Password** retyped. |

**12.** Click **Next**.

**Step Result:** The ***Agent Settings*** page opens.

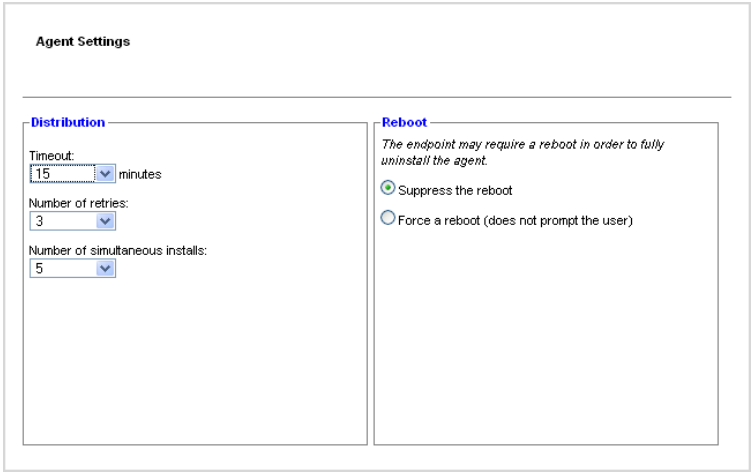



Figure 49: Agent Settings Page

**13.** Define the **Distribution** drop-down lists.

The following table describes each list their available values.

| List | Description |
|---|---|
| **Timeout** | Defines the number of minutes before the agent management job terminates due to a non-responsive agent installation or removal (0-30). |
| **Number of retries** | Defines the number of attempts an agent installation or removal will retry if the initial attempt fails (1-10). |
| **Number of simultaneous installs** | Defines the maximum number of agents that can installed or removed simultaneously during the job (1-25). A value of `1` indicates that serial installs or removals should occur. |

**14.** Define the **Reboot** option.

Select one of the following options:

- **Suppress the reboot**
- **Force a reboot (does not prompt the user)**

**Note:** If the agent being uninstalled is installed on the Lumension Endpoint Management and Security Suite server, the reboot is automatically suppressed regardless of this setting.

**15.** Click **Finish**.

**Result:** The ***Schedule Agent Management Job - Uninstall Wizard*** closes. Depending on how you configured the job, it moves to either the ***Scheduled*** tab or ***Active*** tab on the ***Job Results*** page. The job will run at

the applicable time, uninstalling agents on the defined targets, and move to the ***Completed*** tab when finished.

# Chapter 6

# Reviewing Jobs and Job Results

**In this chapter:**


- About Reviewing Jobs
- The Job Results Page
- The Scheduled Tab
- The Active Tab
- The Completed Tab
- Working with Jobs
- The Results Page
- Working with Results


Following the configuration of discovery scan jobs and agent management jobs, they move to the ***Job Results*** page. This page categorizes jobs based on status. By reviewing and working with jobs, you can view job information or manage the jobs themselves. You can view and edit both discovery scan jobs and agent management jobs from this page.

This page is divided into the following tabs:

- The ***Scheduled*** tab
- The ***Active*** tab
- The ***Completed*** tab

Clicking job names opens detailed information about the jobs.

## About Reviewing Jobs

Following the configuration of a discovery scan job or an agent management job, it moves to the ***Job Results*** page. From this page, you can view jobs before, during, and after activity. Depending on how a job is scheduled during configuration, it will move to either the ***Scheduled*** tab or the ***Active*** tab. Jobs configured to run at a scheduled date and time move to the ***Scheduled*** tab. Jobs configured to run immediately move to the ***Active*** tab.

Jobs on the ***Scheduled*** tab await their activation at the scheduled date and time. Following activation, jobs move to the ***Active*** tab. Any jobs canceled at the ***Scheduled*** tab move to the ***Completed*** tab. Additionally, jobs that recur always appear on this tab until deleted.

Jobs on the ***Active*** tab are performing their intended tasks: discovery scan jobs are detecting and scanning their defined targets, while agent management jobs perform their additional agent management tasks. During activity, you can view partial job results. Job results update as the job progresses and page refreshes. After completion, jobs move to the ***Completed*** tab.

Jobs on the ***Completed*** tab have either been canceled or have finished activity. Once a job moves to the ***Completed*** tab, you can view its complete results. Jobs remain on the ***Completed*** tab until they are deleted.

# The Job Results Page

The ***Job Results*** page is a tabbed page that organizes jobs based on status. Each tab features a list of jobs and a summary of their configurations. Links to each job's ***Results*** page are also available.

**Tip:** You can filter the ***Job Results*** page from the navigation menu:
- Select **Review** > **Job Results** > **Asset Discovery Job Results** to exclusively display discovery scan jobs.
- Select **Review** > **Job Results** > **Agent Management Job Results** to exclusively display agent management jobs.

The ***Job Results*** page contains the following tabs:
- *The Scheduled Tab* on page 139
- *The Active Tab* on page 141
- *The Completed Tab* on page 143

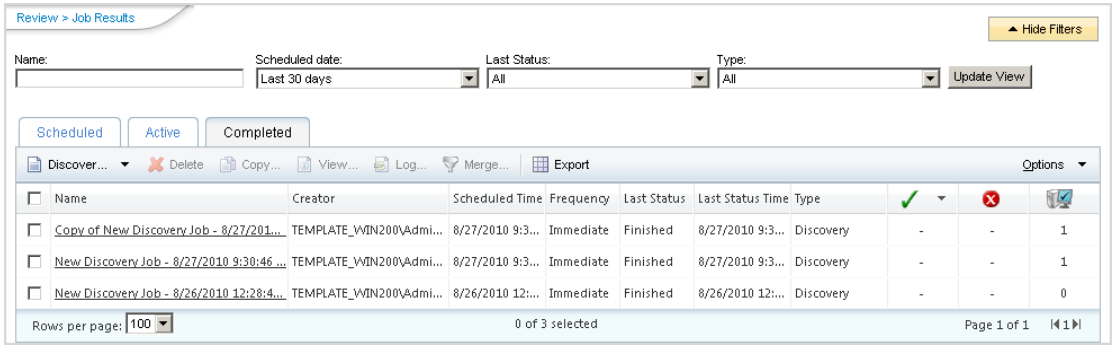



Figure 50: Job Results Page

## Viewing the Job Results Page

Navigate to this page to view the configurations and results of discovery scan jobs and agent management jobs.

You can also use this page to create new jobs.

1. Based on the type of jobs you want to review, select an item from the navigation menu.
   Use one of the following methods to select jobs for review.

| Method | Step |
|---|---|
| **To review discovery scan jobs:** | Select **Review** > **Asset Discovery Job Results**. |
| **To review agent management jobs:** | Select **Review** > **Agent Management Job Results**. |

2. Select the ***Scheduled***, ***Active***, or ***Completed*** tab.
3. If desired, define filter criteria and click **Update View**.

**Result:** The ***Job Results*** page opens to the selected tab.

# The Scheduled Tab

This tab lists pending discovery scan and agent management jobs.

Pending jobs move to the ***Active*** tab at their scheduled dates and times. Additionally, recurring jobs remain listed on this tab until they are canceled or deleted.

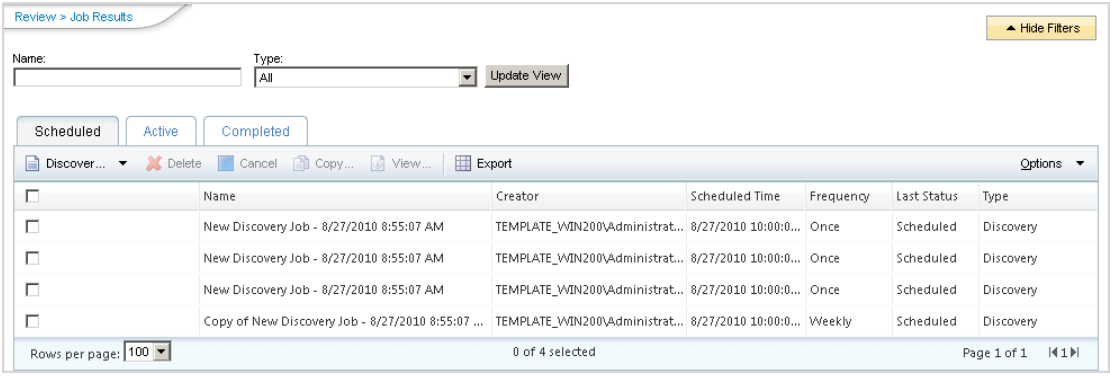



Figure 51: Scheduled Tab

## The Scheduled Tab Toolbar

This toolbar contains buttons related to the creation, viewing, and management of discovery scan jobs and agent management jobs.

Some functions on the ***Scheduled*** tab toolbar are common to all ***Job Results*** page tabs.

Table 51: Scheduled Tab Toolbar

| Button | Function |
|---|---|
| **Discover...**<br>(menu) | Opens the **Discover...** menu. |
| **Assets...**<br>(**Discover ...** menu item) | Creates a custom discovery scan job. For additional information, refer to *Discovering Assets by Discovery Scan Job* on page 97. |
| **Assets and Install Agents...**<br>(**Discover...** menu item) | Installs agents on selected endpoints. For additional information, refer to *Installing Agents by Agent Management Job* on page 111. |
| **Assets and Uninstall Agents...**<br>(**Discover...** menu item) | Deletes agents from selected endpoints. For additional information, refer to *Uninstalling Agents by Agent Management Job* on page 124. |
| **Delete** | Deletes the selected job from the list. For additional information, refer to *Deleting Jobs* on page 148. |

| Button | Function |
|---|---|
| **Cancel** | Cancels the selected job. For additional information, refer to *Canceling Jobs* on page 149. |
| **Copy...** | Duplicates the selected job. For additional information, refer to *Copying Jobs* on page 146. |
| **View...** | Displays the configuration of the selected job. This dialog is read-only. For additional information, refer to *Viewing Job Configurations* on page 147. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |
| **Options** (menu) | Opens the **Options** menu. For additional information, refer to *The Options Menu* on page 31. |

## The Scheduled Tab List

This list contains configuration overviews of scheduled jobs. The number of items in the list depends on how many jobs are pending.

Table 52: Scheduled Tab List

| Column | Description |
|---|---|
| **Name** | The job name. |
| **Creator** | The user account used to create the job. |
| **Scheduled Time** | The scheduled date and time for the job. |
| **Frequency** | The schedule type the job uses (`Once`, `Weekly`, `Monthly`). |
| **Last Status** | The last known status of a job. |
| **Type** | The job type (`Discovery` or `Agent Management`). |

# The Active Tab

This tab lists discovery scan jobs and agent management jobs that are in progress.

The ***Active*** tab also lists active job configuration overviews. Click a job name link to view partial results during job progress. Following completion, active jobs move to the ***Completed*** tab.

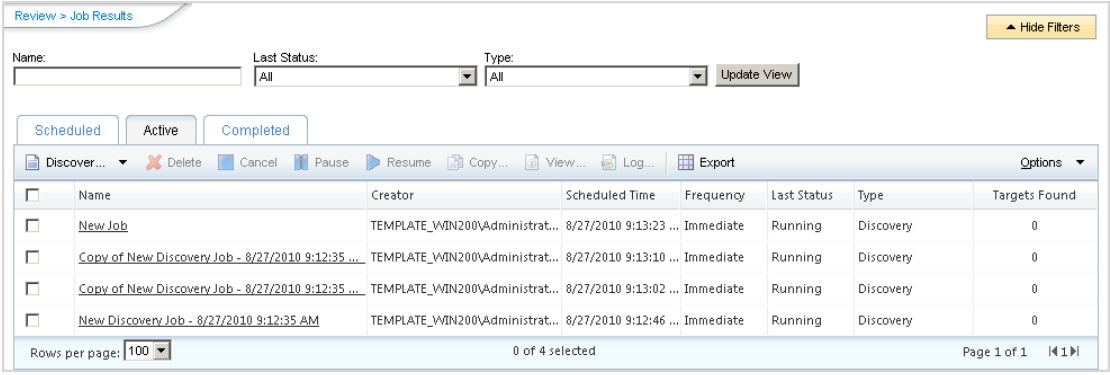



Figure 52: Active Tab

## The Active Tab Toolbar

This toolbar contains buttons related to the creation, viewing, and management of discovery scan jobs and agent management jobs.

Some functions on the ***Active*** tab toolbar are common to all ***Job Results*** page tabs.

Table 53: Active Tab Toolbar

| Name | Function |
|---|---|
| **Discover...**<br>(menu) | Opens the **Discover...** menu. |
| **Assets...**<br>(**Discover ...** menu item) | Creates a custom discovery scan job. For additional information, refer to *Discovering Assets by Discovery Scan Job* on page 97. |
| **Assets and Install Agents...**<br>(**Discover...** menu item) | Installs agents on selected endpoints. For additional information, refer to *Installing Agents by Agent Management Job* on page 111. |
| **Assets and Uninstall Agents...**<br>(**Discover...** menu item) | Deletes agents from selected endpoints. For additional information, refer to *Uninstalling Agents by Agent Management Job* on page 124. |
| **Delete** | Deletes the selected job from the list. For additional information, refer to *Deleting Jobs* on page 148. |

| Name | Function |
|---|---|
| **Cancel** | Cancels the selected job. For additional information, refer to *Canceling Jobs* on page 149. |
| **Pause** | Pauses the selected job. For additional information refer to *Pausing Jobs* on page 151. |
| **Resume** | Continues the selected paused job. For additional information refer to *Resuming a Paused Job* on page 151. |
| **Copy...** | Duplicates the selected job. For additional information, refer to *Copying Jobs* on page 146. |
| **View...** | Displays the configuration of the selected job. This dialog is read-only. For additional information, refer to *Viewing Job Configurations* on page 147. |
| **Log...** | Opens the log for the selected job. For additional information refer to *Viewing a Job Log* on page 149. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |
| **Options** (menu) | Opens the **Options** menu. For additional information, refer to *The Options Menu* on page 31. |

## The Active Tab List

This list contains configuration overviews of active jobs. The number of items in the list depends on how many jobs are active.

The following table describes each list column.

Table 54: Active Tab List

| Column | Description |
|---|---|
| **Name** | The job name. The name is a link to the job's ***Results*** page. |
| **Creator** | The user account used to create the job. |
| **Scheduled Time** | The scheduled date and time for the job. |
| **Frequency** | The schedule type the job uses (`Once`, `Weekly`, `Monthly`). |
| **Last Status** | The last known status of a job. |

| Column | Description |
|---|---|
| **Type** | The job type (`Discovery` or `Agent Management`). |
| **Targets Found** | The number of assets discovered during job activity. |

## The Completed Tab

This tab lists discovery scan jobs and agent management jobs that are completed or canceled, as well as their configuration details.

Completed and canceled jobs remain on this page until you delete them. Additionally, the job name links associated with each completed job take you to that job's ***Results*** page.

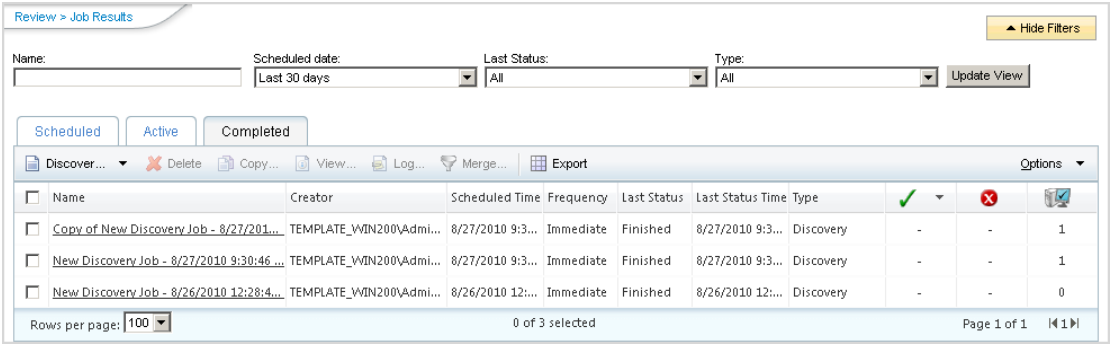



Figure 53: Completed Tab

### The Completed Tab Toolbar

This toolbar contains buttons related to the creation, viewing, and management of discovery scan jobs and agent management jobs.

Some functions on the ***Completed*** tab toolbar are common to all ***Job Results*** page tabs.

Table 55: Completed Tab Toolbar

| Button | Function |
|---|---|
| **Discover...**<br>(menu) | Opens the **Discover...** menu. |
| **Assets...**<br>(**Discover ...** menu item) | Creates a custom discovery scan job. For additional information, refer to *Discovering Assets by Discovery Scan Job* on page 97. |
| **Assets and Install Agents...**<br>(**Discover...** menu item) | Installs agents on selected endpoints. For additional information, refer to *Installing Agents by Agent Management Job* on page 111. |

| Button | Function |
|---|---|
| **Assets and Uninstall Agents...** (**Discover...** menu item) | Deletes agents from selected endpoints. For additional information, refer to *Uninstalling Agents by Agent Management Job* on page 124. |
| **Delete** | Deletes the selected job from the list. For additional information, refer to *Deleting Jobs* on page 148. |
| **Copy...** | Duplicates the selected job. For additional information, refer to *Copying Jobs* on page 146. |
| **View...** | Displays the configuration of the selected job. This dialog is read-only. For additional information, refer to *Viewing Job Configurations* on page 147. |
| **Log...** | Opens the log for the selected job. For additional information refer to *Viewing a Job Log* on page 149. |
| **Merge** | Merges two jobs in to one. For additional information refer to *Merging Jobs* on page 152. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |
| **Options** (menu) | Opens the **Options** menu. For additional information, refer to *The Options Menu* on page 31. |

## The Completed Tab List

This list contains configuration overviews of finished and canceled jobs. The number of items in the list depends on how many jobs are finished and canceled.

The following table describes each list column.

Table 56: Completed Tab Table

| Column | Icon | Description |
|---|---|---|
| **Name** | | The job name. The name is a link to the job's ***Results*** page. |
| **Creator** | | The user account used to create the job. |
| **Scheduled Time** | | The scheduled date and time for the job. |
| **Frequency** | | The schedule type the job uses (`Once`, `Weekly`, `Monthly`). |

| Column | Icon | Description |
|---|---|---|
| **Last Status** | | The last known status of a job. |
| **Last Status Time** | | The date and time of the last status update. |
| **Type** | | The job type (`Discovery` or `Agent Management`). |
| **Total Successful** | | The total number of agents successfully managed (agent management jobs only). |
| **Total Failed** | | The total number of agents that failed to install or uninstall (agent management jobs only). |
| **Total Complete** | | The total number or assets discovered during the scan. |

## Working with Jobs

You can perform a number of tasks related to discovery scan jobs and agent management jobs from the ***Job Results*** page. You can perform most of these tasks regardless of the tab selected. However, certain tasks are specific to certain tabs.

To perform tasks associated with jobs, click a toolbar button. Some buttons are unavailable until one or multiple jobs after selected from the page list.

The following list displays the task that you can perform from the ***Job Results*** page, followed by the tabs that you can perform them from.

- *Discovering Assets* on page 146
- *Installing Agents by Agent Management Job* on page 146
- *Uninstalling Agents by Agent Management Job* on page 146
- *Copying Jobs* on page 146
- *Viewing Job Configurations* on page 147
- *Deleting Jobs* on page 148
- *Exporting Job Result Data* on page 149 tabs)
- *Canceling Jobs* on page 149 (***Scheduled*** and ***Active*** tabs)
- *Viewing a Job Log* on page 149 (***Active*** and ***Completed*** tabs)
- *Viewing Job Results* on page 150 (***Active*** and ***Completed*** tabs)
- *Pausing Jobs* on page 151 (***Active*** tab)
- *Resuming a Paused Job* on page 151 (***Active*** tab)
- *Merging Jobs* on page 152 (***Completed*** tab)

## Discovering Assets

**Discover Assets** jobs are discovery scan jobs that let you customize scheduling, discovery methods, and discovery options. They offer more robust configuration options than their quick-configuration counterparts (discover assets by IP address and discover assets by computer name).

To schedule a discover assets job from any tab on the ***Job Results*** page, select **Discover...** > **Assets...** from the toolbar.

For additional information refer to *Discovering Assets by Discovery Scan Job* on page 97.

## Installing Agents by Agent Management Job

Within Lumension Endpoint Management and Security Suite, you can install agents on endpoints using agent management jobs from multiple pages. These pages include the ***Job Results*** page. To create an agent management job that installs agents from this page, select **Discover...** > **Assets and Install Agents...** from the toolbar.

For additional information, refer to *Installing Agents by Agent Management Job* on page 111.

## Uninstalling Agents by Agent Management Job

Within Lumension Endpoint Management and Security Suite, you can create agent management jobs from multiple pages. These pages include the ***Jobs Results*** page. To create an agent management job that uninstalls agents from this page, select **Discover...** > **Assets and Uninstall Agents...** from the toolbar. You can perform this task from any tab.

For additional information, refer to *Uninstalling Agents by Agent Management Job* on page 124.

## Copying Jobs

On occasion, you may want to create a job (discovery scan or agent management) that is identical to a preexisting completed job. Rather than creating a new job and recreating its configuration, you can copy that preexisting job with the desired configuration values already in place.

Copy jobs from any tab on the **Job Results** page.

1. Based on the type of job you want to copy, select an item from the navigation menu.
   Use one of the following methods to select jobs for copying.

| Method | Step |
|---|---|
| **To copy discovery scan jobs:** | Select **Review** > **Asset Discovery Job Results**. |
| **To copy agent management jobs:** | Select **Review** > **Agent Management Job Results**. |

2. Select the tab that lists the job you want to copy:
   - **Scheduled**
   - **Active**
   - **Completed**

3. Select the check box associated with the job you want to copy.
4. Click **Copy**.

   **Step Result:** Depending on which job you selected, one of the following dialogs opens:

   - ***Copy Discover Assets Job***
   - ***Copy Install Agents Job***
   - ***Copy Uninstall Agents Job***

   The copied job is configured identically to the selected job.

5. If copying an agent management job, dismiss the security credential acknowledgement by clicking **OK**.
6. If desired, edit the job configuration.

   If the job you are copying requires credentials (for either agent management or credential validation), you will have to re-enter the credentials for security purposes.

   **Note:** When editing the ***Copy Discover Assets Wizard***, you can select or clear the **Use existing credential set** check box, which is available on the ***Credentials*** page. This option, which is unavailable during regular discover assets job configuration, lets you retain or discard the credential set entered during source job configuration. If you discard the credential set, you can enter a new credentials set or use no credentials.

7. Click **Save**.

**Result:** The copied job is saved and moved to the applicable ***Job Results*** page tab.

## Viewing Job Configurations

Lumension Endpoint Management and Security Suite can display a job's configuration details in a read-only dialog. View this dialog when you want to see a job's configuration without changing it.

View job configurations from any tab on the ***Job Results*** page.

1. Based on the type of job you want to view, select an item from the navigation menu.

   Use one of the following methods to select jobs for viewing.

| Method | Step |
|---|---|
| **To view discovery scan jobs:** | Select **Review** > **Asset Discovery Job Results**. |
| **To view agent management jobs:** | Select **Review** > **Agent Management Job Results**. |

2. Select the tab that lists the job configuration you want to view:
   - **Scheduled**
   - **Active**
   - **Completed**
3. Select the check box associated with the job you want to view.

4. Click **View**.

**Result:** Depending on the type of job you are viewing, one of the following dialogs opens in a read-only format:

- ***View Discover Assets Job***
- ***View Install Agents Job***
- ***View Uninstall Agents Job***

Use the dialog buttons to scroll through wizard pages.

## Deleting Jobs

When a discovery scan job or an agent management job is no longer necessary, delete that job to completely remove its record from Lumension Endpoint Management and Security Suite. Deleting jobs differs from canceling jobs. Deleted jobs are removed from the ***Job Results*** page altogether; canceled jobs are moved to the ***Completed*** tab.

Delete jobs from any tab on the ***Job Results*** page.

1. Based on the type of job you want to delete, select an item from the navigation menu.
   Use one of the following methods to select jobs for deleting.

| Method | Step |
|---|---|
| **To delete discovery scan jobs:** | Select **Review** > **Asset Discovery Job Results**. |
| **To delete agent management jobs:** | Select **Review** > **Agent Management Job Results**. |

2. Select the tab that lists the job you want to delete.
   - **Scheduled**
   - **Active**
   - **Completed**
3. Select the check box(es) associated with the job(s) you want to delete.
4. Click **Delete**.

   **Step Result:** A dialog appears, asking you acknowledge the deletion.

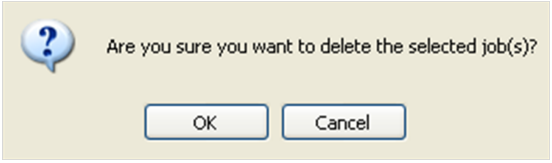



Figure 54: Acknowledge Deletion Dialog

5. Acknowledge the deletion by clicking **OK**.

**Result:** The job is deleted from the list.

## Exporting Job Result Data

To export the list of discovery scan jobs and agent management jobs that are listed on any ***Job Results*** page tab to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information refer to *Exporting Data* on page 37.

## Canceling Jobs

Cancel a discovery scan job or an agent management that you do not want to complete but still want to keep a record of. Canceling jobs differs from deleting jobs. Canceled jobs move to the ***Completed*** tab; deleted jobs are removed from the ***Job Results*** page altogether. You can cancel jobs with a status of scheduled, paused, or running.

Cancel jobs from the ***Scheduled*** and ***Active*** tabs.

1. Based on the type of job you want to cancel, select an item from the navigation menu.
   Use one of the following methods to select jobs for canceling.

| Method | Step |
|---|---|
| **To cancel discovery scan jobs:** | Select **Review** > **Asset Discovery Job Results**. |
| **To cancel agent management jobs:** | Select **Review** > **Agent Management Job Results**. |

2. Select the tab that lists the job(s) you want to cancel:
   - The ***Scheduled*** tab
   - The ***Active*** tab
3. Select the check box(es) associated with the job(s) you want to cancel.
4. Click **Cancel**.

**Result:** The selected job is canceled and moved to the ***Completed*** tab.

## Viewing a Job Log

During activity, jobs record any substantial events or errors that occur. These logs are helpful when troubleshooting network, server, or agent issues. Not all jobs record logs.

View job logs from the ***Active*** or ***Completed*** tabs. Active job logs may not be complete because scanning or agent installation is not finished.

1. Based on the type of job log you want to view, select an item from the navigation menu.
   Use one of the following methods to select job logs for viewing.

| Method | Step |
|---|---|
| **To view discovery scan job logs:** | Select **Review** > **Asset Discovery Job Results**. |

| Method | Step |
|---|---|
| **To view agent management job logs:** | Select **Review** > **Agent Management Job Results**. |

2. Select the tab that lists the job containing the log you want to view:
   - the ***Active*** tab
   - the ***Completed*** tab
3. Select the check box associated with the job containing the log you want to view.
4. Click **Log**.

**Note:** If more than one job is selected, or if the selected job does not have a log, then **Log** is unavailable.

**Result:** The ***Job Log Details*** dialog opens.

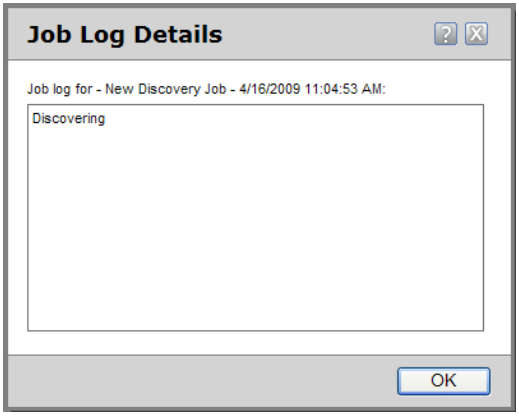



Figure 55: Job Log Details Dialog

## Viewing Job Results

You can see the results for a job after it completes or while it runs. However, viewing the results for an active job will display only partially completed results. View results by clicking job name links, which open the applicable job's ***Results*** page.

Access job results from the ***Active*** and ***Completed*** tabs.

1. Based on the type of job results you want to view, select an item from the navigation menu.

   Use one of the following methods to select job results for viewing.

| Method | Step |
|---|---|
| **To view results for discovery scan jobs:** | Select **Review** > **Asset Discovery Job Results**. |

| Method | Step |
|---|---|
| **To view results for agent management jobs:** | Select **Review** > **Agent Management Job Results**. |

2. Select the tab that lists the job for which you want to view results:
   - **Active**
   - **Completed**
3. Click the job name link for the job results you want to view.

**Note:** Scheduled jobs have no job name links.

**Result:** The ***Results*** page for the job you selected opens. The ***Results*** page for active jobs is partially complete because the job is still active. More job information appears as you refresh the page.

## Pausing Jobs

While discovery scan jobs or agent management jobs are active, they can be temporarily paused. Only active jobs can be paused.

Pause jobs from the ***Active*** tab.

1. Based on the type of job you want to pause, select an item from the navigation menu.
   Use one of the following methods to select jobs for pausing.

| Method | Step |
|---|---|
| **To pause discovery scan jobs:** | Select **Review** > **Asset Discovery Job Results**. |
| **To pause agent management jobs:** | Select **Review** > **Agent Management Job Results**. |

2. Select the ***Active*** tab.
3. Select the check box(es) associated with the job(s) you want to pause.
4. Click **Pause**.

**Result:** The selected job is paused.

## Resuming a Paused Job

Resume paused jobs to continue their activity. Only paused jobs can be resumed.

Resume paused jobs from the ***Active*** tab.

1. Based on the type of job you want to resume, select an item from the navigation menu.
   Use one of the following methods to select jobs for resuming.

| Method | Step |
|---|---|
| **To resume discovery scan jobs:** | Select **Review** > **Asset Discovery Job Results**. |

| Method | Step |
|---|---|
| **To resume agent management jobs:** | Select **Review** > **Agent Management Job Results**. |

2. Select the ***Active*** tab.
3. Select the check box(es) associated with the paused job(s) you want to resume.
4. Click **Resume**.

**Result:** The selected job resumes activity.

## Merging Jobs

Merging completed jobs lets you view the results for two different jobs on one page. This feature is convenient for when you want to review multiple jobs' results without having to navigate between jobs. You can only merge completed jobs.

Merge completed jobs from the ***Completed*** tab. You can merge an unlimited number of completed jobs.

**Note:** Agent management jobs that install agents and agent management jobs that uninstall agents cannot be merged.

1. Based on the type of jobs you want to merge, select an item from the navigation menu.

   Use one of the following methods to select jobs for merging.

| Method | Step |
|---|---|
| **To merge discovery scan jobs:** | Select **Review** > **Asset Discovery Job Results**. |
| **To merge agent management jobs:** | Select **Review** > **Agent Management Job Results**. |

2. Select the ***Completed*** tab.
3. Select the check boxes associated with the jobs you want to merge.

4. Click **Merge**.

   **Step Result:** The ***Merge Jobs*** dialog opens.

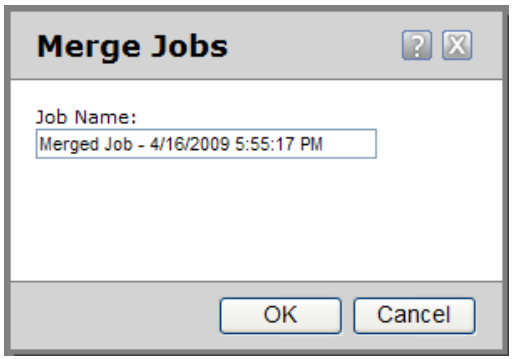



Figure 56: Merge Jobs Dialog

5. If desired, type a new name for the job in the **Job Name** field.

   **Note:** By default, new merged jobs are named `Merged Job`, followed by the server-side date and time, formatted according to the server's locale setting.

6. Click **OK**.

**Result:** The merged job appears in the list.

## The Results Page

This page lists the results for a selected discovery scan job or agent management job. Particularly, it lists each endpoint found during scanning, the endpoints' operating systems, and their address information. When the viewed ***Results*** page is associated with an agent management job, additional information about agent information is displayed. Use this page to determine candidates for agent installation or to verify that an agent management job ran smoothly.

You can access a job's ***Results*** page by clicking the links listed on the ***Job Results*** page ***Active*** and ***Completed*** tabs. However, if you access a ***Results*** page while a job is still active, the results will be incomplete.

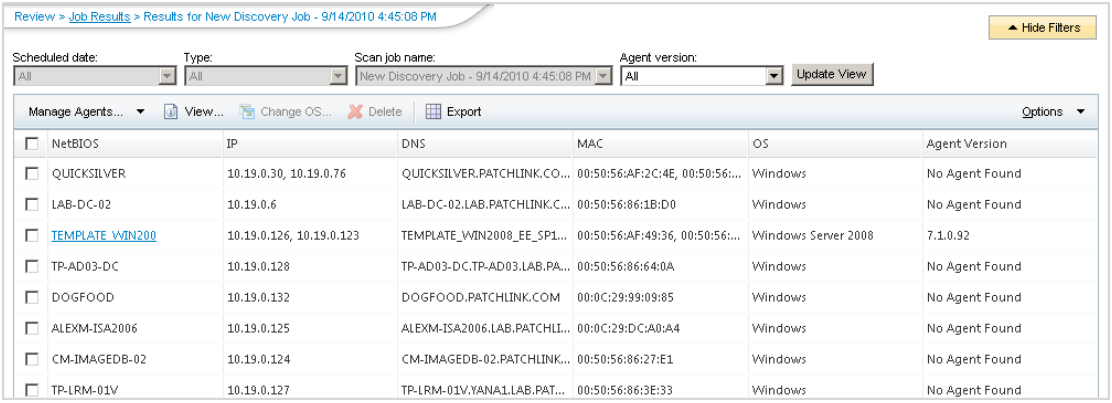



Figure 57: Results Page

**Note:** The ***Results*** page *is not* the ***Job Results*** page. The ***Results*** page contains endpoint details, while the ***Job Results*** page contains job configuration details. For additional information about the ***Job Results*** page, refer to *The Job Results Page* on page 138.

## Viewing the Results Page

After running a discovery scan job or agent management job, you can view detailed results for individual jobs.

View the ***Results*** page by clicking a job link from the ***Job Result***s page.

1. Depending on the job results you want to view, select one of the following menu items:
   - **Review** > **Asset Discovery Job Results**
   - **Review** > **Agent Management Job Results**
2. Select the tab containing the job you want to review results for.
   - The ***Active*** tab
   - The ***Completed*** tab
3. Click the job link for the results you want to review.

**Result:** The ***Results*** page for the selected job opens.

## The Results Page Toolbar

This toolbar contains buttons for features related to job results for endpoints.

The following table describes ***Results*** page toolbar button functions.

Table 57: Results Page Toolbar

| Button | Function |
|---|---|
| **Manage Agents...** (menu) | Opens the **Manage Agents** menu. |

| Button | Function |
|---|---|
| **Install Agents...**<br>(**Manage Agents...** menu item) | Installs agents on selected endpoints. For additional information, refer to *Installing Agents by Agent Management Job* on page 111. |
| **Uninstall Agents...**<br>(**Manage Agents...** menu item) | Uninstalls agents from selected endpoints. For additional information, refer to *Uninstalling Agents by Agent Management Job* on page 124. |
| **Download Agent Installer...**<br>(**Manage Agents...** menu item) | Downloads an agent installer to the endpoint used to access Lumension Endpoint Management and Security Suite. For additional information, refer to *Downloading the Agent Installer* on page 166. |
| **View...** | Displays the configuration of the selected job. This dialog is read-only. For additional information, refer to *Viewing Job Configurations* on page 147. |
| **Change OS** | Changes the operating system result for the selected endpoint. For additional information refer to *Changing Endpoint Operating System Results* on page 158. |
| **Delete** | Deletes the selected endpoint result from the list. For additional information refer to *Deleting Job Endpoint Results* on page 159. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |
| **Options**<br>(menu) | Opens the **Options** menu. For additional information, refer to *The Options Menu* on page 31. |

## The Results Page List

This list itemizes all endpoints discovered during the selected job. It also displays endpoint agent, address, and operating system information. Endpoints with agents installed offer links to their ***Details*** page.

The following table displays the information found on the ***Results*** page list.

Table 58: Results Page List

| Column | Description |
|---|---|
| **Access Level** | The access level that the credentials entered during job configuration achieved on the endpoint (`No Access`, `Read`, `Full`, `Agent Installed`). For addition information refer to *Access Levels* on page 157.<br>**Note:** This column only appears for agent management jobs or discovery scan jobs that had the **Validate credential access level** option selected. |
| **NetBIOS** | The NetBIOS name of the endpoint. The name serves as a link to the ***Details*** page for endpoints that have agents installed. |
| **IP** | The IP address of the endpoint. |
| **DNS** | The DNS name of the endpoint. |
| **MAC** | The MAC address of the endpoint. |
| **OS** | The operating system of the endpoint. |
| **Install Status** | The status of an agent installation.<br>**Note:** This column only appears if the ***Results*** page pertains to an agent management job or a merged job containing an agent management job. |
| **Status Message** | The explanation of the **Install Status**.<br>**Note:** This column only appears if the ***Results*** page pertains to an agent management job or a merged job containing an agent management job. |
| **Agent Version** | The agent version installed on the endpoint. A `No Agent Found` value indicates either no agent is present or the agent could not be detected. |

**Note:** Endpoint results are collected during job activity. Therefore, older jobs may contain obsolete information. Additionally, if agent management jobs are failing, their target endpoints may not be properly configured. For additional information of configuring endpoints for agent management jobs, refer to the following topics:

- *Configuring Endpoints for Agent Management Jobs (Pre-Windows Vista)* on page 326
- *Configuring Endpoints for Agent Management Jobs (Post-Windows Vista)* on page 334

### Access Levels

The ***Results*** page also displays the **Access Level** column for agent management jobs and discovery jobs that have had the **Validate credential access level** option selected. This column displays the access levels that job credentials permit for job targets. Access levels provide feedback as to whether credentials entered during job configuration can provide agent management permission.

The following table describes each access level.

Table 59: Access Levels

| Access Level | Description |
|---|---|
| `None` | Indicates the endpoint was discovered, but the credentials entered during job configuration are invalid on the applicable endpoint. |
| `Read` | Indicates the credentials entered during job configuration provide read access to the applicable endpoint's share drives. These credentials provide the access rights needed to run agent management jobs. |
| `Full` | Indicates the credentials entered during job configuration have read and write access to the applicable endpoint's share drives. These credentials provide the access rights needed to run agent management jobs. |
| `Agent Installed` | Indicates that the endpoint has an agent installed. |

## Working with Results

To perform tasks associated with job results, click a toolbar button. To perform some tasks, selecting one or multiple jobs from the ***Results*** page may be necessary.

- *Viewing Endpoint Details* on page 157
- *Installing Agents by Agent Management Job* on page 111
- *Uninstalling Agents by Agent Management Job* on page 124
- *Installing an Agent* on page 165
- *Changing Endpoint Operating System Results* on page 158
- *Deleting Job Endpoint Results* on page 159
- *Exporting Discovery Scan Result Data* on page 160

### Viewing Endpoint Details

The ***Results*** page features links to the ***Details*** page for endpoints that have agents installed. View endpoint ***Details*** pages when you want to view agent-collected data about an endpoint. Links are not available for endpoints without agents installed.

You can also access endpoint details from the ***Endpoints*** page.

1. Depending on the job results you want to view, select one of the following menu items:
   - **Review** > **Asset Discovery Job Results**

- **Review** > **Agent Management Job Results**

2. Ensure the **Active** or the ***Completed*** tab is selected.
3. Click the desired job name link.

   **Step Result:** The ***Results*** page for the selected job opens.

4. Click the desired NetBIOS link.

   **Note:** NetBIOS links are only available for endpoints with agents installed.

**Result:** The ***Details*** page for the selected endpoint opens.

## Installing Agents by Agent Management Job

Within Lumension Endpoint Management and Security Suite, there are multiple methods of installing agents on endpoints using agent management jobs. To create an agent management job that installs agents from the ***Results*** page, select **Manage Agents** > **Install Agents** from the toolbar.

For additional information refer to *Installing Agents by Agent Management Job* on page 111.

## Uninstalling Agents by Agent Management Job

Within Lumension Endpoint Management and Security Suite, there are multiple methods of uninstalling agents from endpoints using agent management jobs. To create an agent management job that uninstalls agents from the ***Results*** page, select **Manage Agents** > **Uninstall Agents** from the toolbar.

For additional information refer to *Uninstalling Agents by Agent Management Job* on page 124.

## Downloading the Agent Installer

From the ***Results*** page, you can download an agent installer to the endpoint that you are using.

To download an agent installer from the ***Results*** page, select **Manage Agents** > **Download Agent Installer** from the toolbar. For additional information refer to *Downloading the Agent Installer* on page 166.

## Changing Endpoint Operating System Results

When a job does not have the scan options selected necessary to identify an endpoint's operating system, Lumension Endpoint Management and Security Suite identifies the endpoint's operating system as generic or unknown. When this event occurs, you can correct an endpoint's operating system scan result manually.

Change the operating system result of an endpoint from the ***Results*** page.

1. Select one of the following items from the navigation menu.
   - **Review** > **Asset Discovery Job Results**
   - **Review** > **Agent Management Job Results**

   These menu items filter the ***Job Results*** page for the selected job type.
2. Ensure the ***Completed*** tab is selected.
3. Click the desired job name link.

   **Step Result:** The ***Results*** page for the selected job opens.

4. Select the check box(es) associated with the operating system result(s) you want to change.
5. Click **Change OS**.

   **Step Result:** The ***Change OS*** dialog opens.

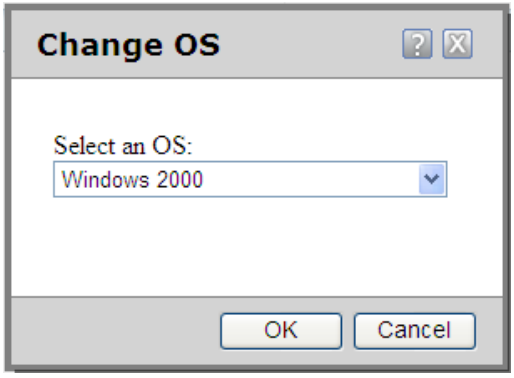



Figure 58: Change OS Dialog

6. Select the desired operating system from the list.
7. Click **OK**.

**Result:** The selected operating system result is changed.

## Deleting Job Endpoint Results

While viewing results for a selected discovery scan job or agent management job, you can delete the entry for any endpoint scanned during the job. Delete entries when you no longer need them; for example, when an endpoint is removed from the network.

Delete endpoint entries from a job's ***Results*** page.

1. Select one of the following items from the navigation menu.
   - **Review** > **Asset Discovery Job Results**
   - **Review** > **Agent Management Job Results**

   These menu items filter the ***Job Results*** page for the selected job type.
2. Select the ***Completed*** tab.
3. Click a job name link.

   **Step Result:** The job's ***Results*** page opens.
4. Select the check box(es) associated with the results you want to delete.
5. Click **Delete**.

   **Step Result:** A dialog displays, asking you to acknowledge the deletion.
6. Click **OK**.

**Result:** The selected discovery scan results are deleted from the list.

## Exporting Discovery Scan Result Data

To export the list of endpoints that are listed on the ***Results*** page to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analysis purposes.

For additional information refer to *Exporting Data* on page 37.

# Chapter 7

# Using Endpoints

**In this chapter:**


- About Endpoints
- The Endpoints Page
- Working with the Endpoints Page
- The Endpoint Details Page
- Working with the Endpoint Details Page


While using Lumension Endpoint Management and Security Suite (Lumension EMSS), you can view and manage network endpoints after installing agents. You can also view the inventory on each endpoint.

The ***Endpoints*** page contains a listing of all endpoints that have an agent registered with the Lumension EMSS. From this list of endpoints, you can access the endpoint details. The endpoint details include endpoint-specific information.

## About Endpoints

The ***Endpoints*** page is used to manage the computers and devices on your network. Endpoint management describes the process by which the Lumension Endpoint Management and Security Suite (Lumension EMSS) server queues commands that will be sent to the endpoint using the agent. When the agent contacts the server, the commands are executed.

The ***Endpoints*** page lists all endpoints registered to the Lumension EMSS. The page displays general information about the endpoint, such as the endpoint name, status, operating system, and agent version.

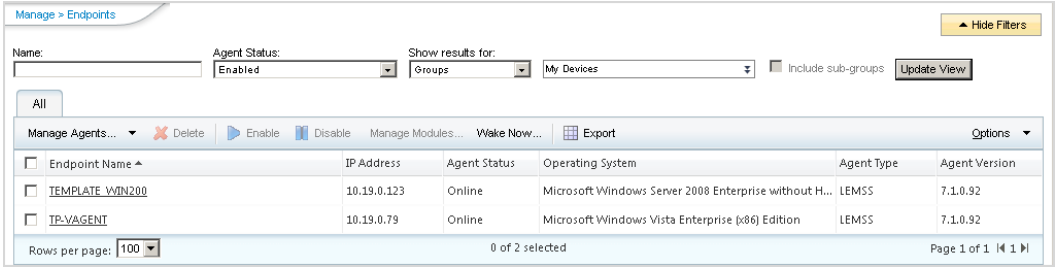



Figure 59: Endpoints Page

### Viewing the Endpoints Page

The ***Endpoints*** page has filters that allow you to customize your view of the computers and other devices that are managed on your network.

1. Select **Manage** > **Endpoints**.

2. Select your filter options.
3. Click **Update View**.

**Result:** The ***Endpoints*** page displays the endpoints that match the selected filter options.

**Note:** To view all endpoints, select the **Include Sub-Groups** check box.

# The Endpoints Page

The ***Endpoints*** page contains information about the managed endpoints on your network. From the ***Endpoints*** page, you can use features associated with endpoints.

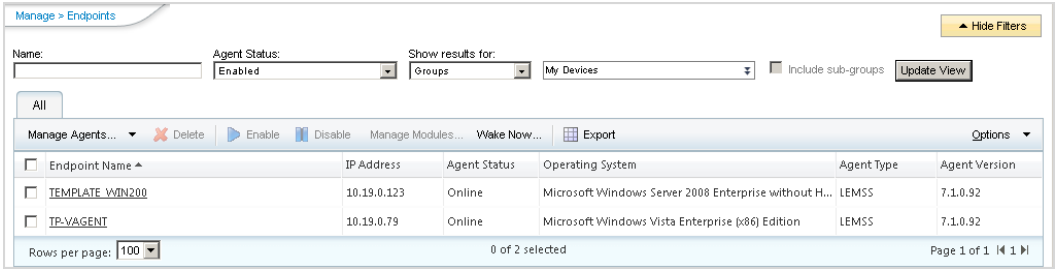



Figure 60: Endpoints Page

## The All Tab

This tab lists information about endpoints, the agent version installed on them, and the module features active on them.

This tab displays by default when you open the ***Endpoints*** page.

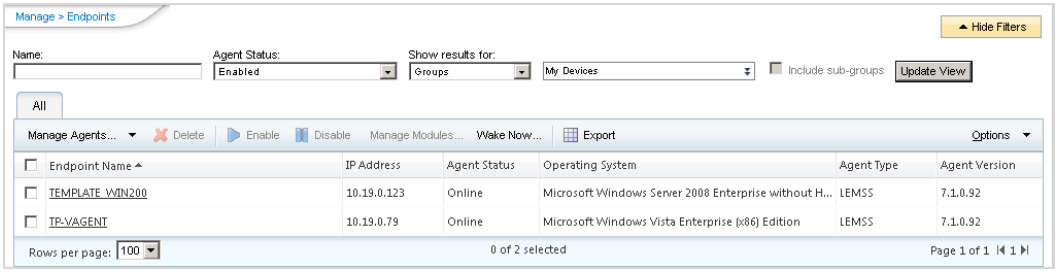



Figure 61: All Tab

### The All Tab Toolbar

The ***All*** tab toolbar contains the tasks and functions that are available for you to perform for managed endpoints.

The following table describes the toolbar functions used in the ***Endpoints*** page.

Table 60: All Tab Toolbar Functions

| Button | Function |
|---|---|
| **Manage Agents...** (menu) | Opens the **Manage Agents** menu. |
| **Install Agents...** (**Manage Agents...** menu item) | Installs agents on selected endpoints. For additional information, refer to *Installing Agents by Agent Management Job* on page 111. |
| **Uninstall Agents...** (**Manage Agents...** menu item) | Uninstalls agents from selected endpoints. For additional information, refer to *Uninstalling Agents by Agent Management Job* on page 124. |
| **Download Agent Installer...** (**Manage Agents...** menu item) | Downloads an agent installer to the endpoint used to access Lumension Endpoint Management and Security Suite. For additional information, refer to *Downloading the Agent Installer* on page 166. |
| **Agent Versions...** | Defines the agent version(s) that can be installed on an endpoint. For additional information, refer to *Defining the Endpoint Agent Version* on page 166. |
| **Delete** | Deletes a disabled endpoint. For additional information, refer to *Deleting an Endpoint* on page 167. |
| **Enable** | Enables a disabled endpoint. For additional information, refer to *Enabling an Endpoint* on page 168.<br>**Note:** This button is only available when an endpoint is disabled. |
| **Disable** | Disables an enabled endpoint. For additional information, refer to *Disabling an Endpoint* on page 169. |
| **Manage Modules...** | Opens the **Add/Remove Modules** dialog. Use this dialog to toggle module-specific agent functions. For additional information, refer to *Managing Module Endpoint Components* on page 170. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |

| Button | Function |
|---|---|
| **Options** | Opens the **Options** menu. For more information, see *The Options Menu* on page 31. |

## The All Tab List

The ***All*** tab list itemizes endpoint operating system information, identification information, agent information, and module information.

The following table describes the columns within the ***All*** tab list.

Table 61: All Tab List Columns

| Column | Description |
|---|---|
| **Name** | Indicates the name of the endpoint. Clicking the ***Name*** link displays the applicable ***Endpoint Details*** page. See *The Endpoint Details Page* on page 171 for additional information. |
| **IP Address** | Indicates the IP address of the endpoint. |
| **Agent Status** | Indicates the status of the endpoint (`Online`, `Offline`, or `Disabled`). |
| **Operating System** | Indicates the operating system the endpoint is running. |
| **Agent Type** | Indicates the type of agent that is running on the endpoint and communicating with the Lumension Endpoint Management and Security Suite server. |
| ***Module*** **Installed** | Indicates whether a component module is installed on the endpoint. A ***Module*** **Installed** column appears for each component module installed on your Lumension Endpoint Management and Security Suite server. The following list defines column entry values:<br>**Yes** — The module is installed.<br>**Pending** — The module is pending install or uninstall.<br>**No** — The module is not installed.<br>**Error** — There was an error while installing or uninstalling the module. Click the error link for additional information about the error.<br>**Expired** — The module license has expired. |

# Working with the Endpoints Page

You can perform a number of tasks related to endpoints using toolbar buttons on the ***Endpoints*** page. Certain tasks are specific to certain tabs.

Click a button to perform a task. Some buttons are not available until one or more list item is selected.

The following list displays the tasks that you can perform from the ***Endpoints*** page, followed by the tabs that you can perform them from.

- *Installing an Agent* on page 165 (***All*** tab)
- *Installing Agents by Agent Management Job* on page 165 (***All*** tab)
- *Uninstalling Agents by Agent Management Job* on page 165 (***All*** tab)
- *Downloading the Agent Installer* on page 166 (***All*** tab)
- *Defining the Endpoint Agent Version* on page 166 (***All*** tab)
- *Deleting an Endpoint* on page 167 (***All*** tab)
- *Enabling an Endpoint* on page 168 (***All*** tab)
- *Disabling an Endpoint* on page 169 (***All*** tab)
- *Managing Module Endpoint Components* on page 170 (***All*** tab)

## Installing an Agent

Installing an agent on the Lumension Endpoint Management and Security Suite (Lumension EMSS) server is required to manage endpoints.

There are two ways in which you can install an agent on an endpoint:

- Install an agent locally by browsing to the Lumension EMSS server from the endpoint that you want to manage and downloading the agent installer. For additional information, refer to *Downloading the Agent Installer* on page 166.
- Install an agent remotely by creating an agent management job. For additional information, refer to *Installing Agents by Agent Management Job* on page 111.

## Installing Agents by Agent Management Job

Within Lumension Endpoint Management and Security Suite, there are multiple methods of installing agents from endpoints using agent management jobs. To create an agent management job that installs agents from the ***Endpoints*** page, select **Manage Agents... > Install Agents...** from the toolbar.

**Tip:** You can predefine job targets by selecting endpoints from the page list.

For additional information refer to *Installing Agents by Agent Management Job* on page 111.

## Uninstalling Agents by Agent Management Job

Within Lumension Endpoint Management and Security Suite, there are multiple methods of uninstalling agents from endpoints using agent management jobs. To create an agent management job that uninstalls agents from the ***Endpoints*** page, select **Manage Agents... > Uninstall Agents...** from the toolbar.

**Tip:** You can predefine job targets by selecting endpoints from the page list.

For additional information, refer to *Uninstalling Agents by Agent Management Job* on page 124.

## Defining the Endpoint Agent Version

From the ***Endpoints*** page, you define which version(s) of the Lumension Endpoint Management and Security Suite Agent can be installed on the selected endpoint.

Define agent version(s) for selected endpoints from any ***Endpoints*** page tab.

1. Select **Manage** > **Endpoints**

   **Step Result:** The ***Endpoints*** page opens to the ***All*** tab.

2. Select the endpoints on which you want to define agent version(s).
3. Click **Agent Versions...**.

   **Step Result:** The ***Manage Agent Versions*** dialog opens.

4. Define the agent version(s).
   Use one of the following methods:

| Method | Steps |
|---|---|
| **To define a standard agent version for all listed endpoints:** | • From the **Select One** list, select an agent version.<br>• Click **Apply to All Agents**. |
| **To define an agent version for each endpoint:** | Select an agent version from the **Agent Version** list for each endpoint. |

**Note:** The agent versions available for selections are defined from the ***Options*** page. For additional information, refer to *Configuring the Agents Tab* on page 80.

5. Click **OK**.

**Result:** The ***Manage Agent Versions*** dialog closes. If an agent version other than the defined version is installed on the endpoints, the defined version is installed over the previous version.

## Downloading the Agent Installer

You can install an agent locally by connecting to the Lumension Endpoint Management and Security Suite (Lumension EMSS) server, downloading the agent installer, and running the installer on the endpoint that you want to manage.

The following procedure describes the steps required to download the agent installer to the endpoint that you want to manage using Lumension EMSS. The agent system requirements and installation procedure varies by operating system. For complete instructions regarding the installation of agents on supported operating systems, refer to the *Lumension Endpoint Management and Security Suite 7.1 Agent Installation Guide* (*http://portal.lumension.com*).

1. Log on to the target computer as the local administrator (or a member of the **Local Administrators** group).
2. Log into your Lumension Endpoint Management and Security Suite server.

3. From the toolbar, select **Tools** > **Download Agent Installer...**.

   **Step Result:** The ***Download Agent Installers*** dialog displays.

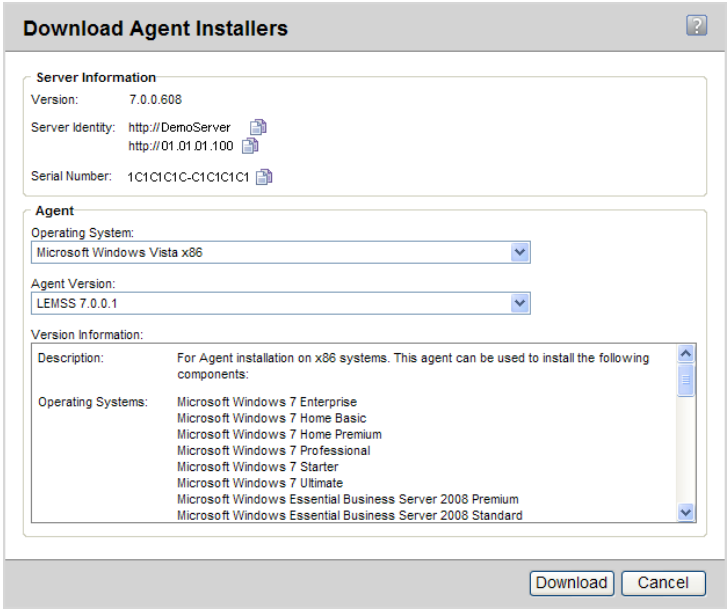



Figure 62: Agent Installer

4. Select the endpoint's operating system from the **Operating System** drop-down list.
5. Select the agent version that you want to install on the endpoint from the **Agent Version** drop-down list.

   **Note:** The agent versions available for selection are defined by the **Agent Version Options**, which you can edit from the ***Options*** page ***Agents*** tab. For additional information, refer to *Agent Versions* on page 77.

6. Click **Download**.

**Result:** A ***Download File*** dialog opens, prompting you to save or open the installer.

## Deleting an Endpoint

Deleting an endpoint removes it from the list of managed endpoints in Lumension Endpoint Management and Security Suite.

Delete endpoints from the ***Endpoints*** page ***All*** tab.

1. Select **Manage** > **Endpoints**.
2. Select one or multiple endpoints with disabled agents.

   **Note:** You can only delete disabled agents. For additional information, refer to *Disabling an Endpoint* on page 169.

3. In the toolbar, click **Delete**.

   **Step Result:** A ***delete confirmation*** dialog displays.

4. Click **OK** to confirm the deletion.

**Result:** The endpoint is deleted from the list.

## Enabling Modules on Endpoint

Enabling a module's endpoint component activates the module functions for the endpoint's agent after they have been disabled.

**Prerequisites:**

Endpoints must have the applicable agent module installed, and the endpoint must be licensed for the agent module. For additional information, refer to *Managing Module Endpoint Components* on page 170.

Enable a module from the applicable ***Endpoints*** page tab.

1. Select **Manage** > **Endpoints**.
2. Select the tab for the module that you want to enable for an endpoint.
3. Select one or more endpoint that does not have the module enabled.
4. From the toolbar, select **Enable** > **Enable Module**.

**Result:** The module for the selected endpoints is enabled.

## Enabling an Endpoint

Enabling an endpoint includes the endpoint in the content management activities of the Lumension Endpoint Management and Security Suite.

Enable endpoints from the ***Endpoints*** page (any tab).

1. Select **Manage** > **Endpoints**.
2. Enable the endpoint(s) by completing a set of substeps.

| Context | Steps |
|---|---|
| **To enable endpoints from the *All* tab:** | 1. Ensure the ***All*** tab is selected.<br>2. Select the disabled endpoint(s) you want to enable.<br>3. Click **Enable**. |

**Result:** The agent and all modules are enabled.

## Disabling Modules on Endpoint

Disabling a module's endpoint components deactivates the module functions for the endpoint's agent and releases a license for the module.

Disable a module from the applicable ***Endpoints*** page tab.

**Note:** You can only disable enabled modules.

1. Select **Manage** > **Endpoints**.
2. Select the tab for the module that you want to disable for an endpoint.
3. Select one or more endpoints with the agent module enabled.

4. From the toolbar, select **Disable** > **Disable Module**.

   **Step Result:** A notification displays, informing you that disabling the module stops module-related functions.

5. Click **OK** to dismiss the notification.

**Result:** The module for the selected endpoints is disabled.

## Disabling an Endpoint

Once an endpoint is disabled, the installed modules no longer function.

Disable endpoints from the ***Endpoints*** page (any tab).

1. Select **Manage** > **Endpoints**.
2. Perform one of the following substep sets based on your context.

| Context | Steps |
|---|---|
| **To disable endpoints from the *All* tab:** | 1. Ensure the ***All*** tab is selected.<br>2. Select the disabled endpoint(s) you want to enable.<br>3. Click **Disable**. |

**Result:** The endpoint is displayed in the list of endpoints identified with the disabled icon in the **Status** column. After disabling an agent, the endpoint can be deleted from Lumension Endpoint Management and Security Suite.

**Note:** Once disabled, the endpoint may not appear in the list based on the **Status** filter settings. To include disabled endpoints in the list, ensure you select **Disabled** or **All** in the **Status** filter.

## The Add/Remove Modules Dialog

This dialog lists information about each module license you have purchased. You can also use it to install or remove module endpoint components within your network.

Open this dialog from the ***Endpoints*** page by selecting one endpoint or more and clicking **Manage Modules...**.

The following describes each item in the dialog table.

Table 62: Add/Remove Dialog Table

| Item | Description |
|---|---|
| **Licenses** | The modules you are currently licensed for. A column appears for each module you are licensed for. |
| **Purchased** | The number of licenses purchased for the applicable module. |
| **In Use** | The number of licenses in use for the applicable module. |
| **Pending** | The number of licenses pending installation or removal for the applicable module. |
| **Available** | The number of module licenses available for assignment. |

The following table describes each column in the dialog list.

Table 63: Add/Remove Dialog List

| Column | Description |
|---|---|
| **Endpoint Name** | Indicates the name of managed endpoint. |
| **IP Address** | Indicates the IP address of the managed endpoint. |
| **Agent Version** | Indicates the agent version number defined for the endpoint. |
| ***Module Name***<br>**Note:** There is a ***Module Name*** column for each module you have purchased. | Indicates if the module endpoint component for the applicable module is installed on the endpoint. A selected check box indicates the component is installed on the endpoint. A cleared check box indicates the module is not installed on the endpoint. |

### Managing Module Endpoint Components

Before you can use a module's functions on your Lumension Endpoint Management and Security Suite network endpoints, you must first install the module's endpoint component on the applicable endpoints. After installing a module endpoint, you can remove it any time.

**Prerequisites:**

If installing a module's endpoint components, the module's server component must be installed.

Manage module endpoint components for individual endpoints from the ***Add/Remove Modules*** dialog.

1. Select **Manage** > **Endpoints**.
2. Select the checkbox(es) associated with the endpoints for which you want to manage modules.
3. Click **Manage Modules...**.

   **Step Result:** The ***Add/Remove Modules*** dialog opens.

4. Manage modules for each endpoint.
   - To add a module for a particular endpoint, select the module checkbox for the applicable endpoint.
   - To remove a module for a particular endpoint, clear the module checkbox for the applicable endpoint.

   **Tip:** Select or clear the **Select All** check box(es) associated with a module to globally toggle a module for all endpoints. Endpoints with unsupported OSs or agents that do not support the module cannot be selected.

5. Click **OK**.

**Result:** The ***Add/Remove Modules*** dialog closes. The agent features for each edit are updated during the next Discover Applicable Updates task.

## Exporting Endpoint Information

You can export the endpoint information generated in the Lumension Endpoint Management and Security Suite so that it can be used in other applications.

The export utility lets you export endpoint information to a comma-separated value (`.CSV`) file format. For additional information, refer to *Exporting Data* on page 37.

# The Endpoint Details Page

The ***Endpoint Details*** page provides endpoint-specific information. The tabs access specific details about the endpoint.

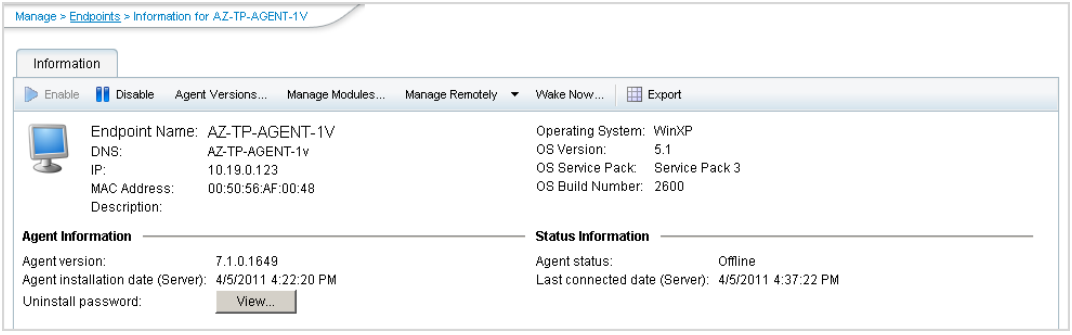



Figure 63: Endpoint Details Page

## Viewing the Endpoint Details Page

The ***Endpoint Details*** page contains comprehensive details for an endpoint and its activity within the Lumension Endpoint Management and Security Suite system.

View the ***Endpoint Details*** page for an endpoint by clicking an endpoint name link from the ***Endpoints*** page.

1. Select **Manage** > **Endpoints**.

   **Step Result:** The ***Endpoints*** page opens to the ***All*** tab.

2. Click the **Name** link associated with the endpoint details you want to review.

   **Step Result:** The ***Endpoint Details*** page opens to the ***Information*** tab.

3. If desired, select a page tab.

   The page tabs available differ according to the modules installed on your server.

## The Information Tab

The ***Information*** tab displays important information about the endpoint. The page displays general information organized into endpoint, agent, status, component, group, and policy sections.

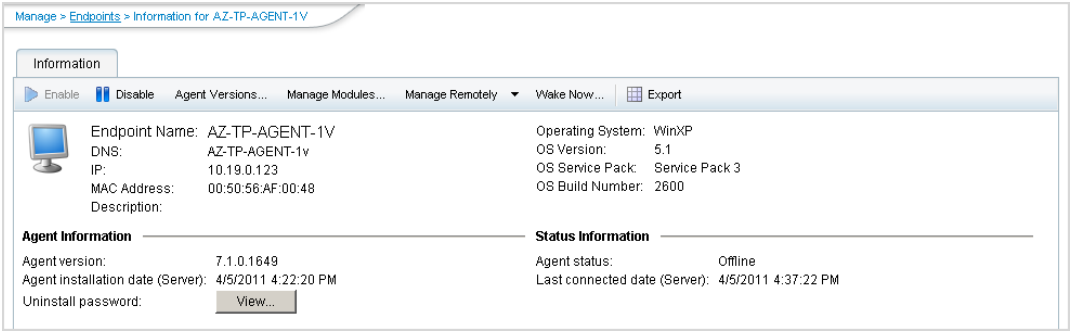



Figure 64: The Information Tab

### The Information Tab Toolbar

The ***Information*** tab toolbar contains the endpoint assessment tasks and functions that are available for you to perform on managed endpoints.

The following table describes the buttons available in the ***Information*** tab toolbar.

Table 64: Information Tab Toolbar Buttons

| Toolbar Button | Description |
|---|---|
| **Agent Versions...** | Defines the agent version(s) that can be installed on an endpoint. For additional information, refer to *Defining the Endpoint Agent Version (Endpoint Details)* on page 181. |
| **Enable** | Enables the endpoint (if it is disabled). For additional information, refer to *Enabling an Endpoint* on page 181. |
| **Disable** | Disables the endpoint (if it is enabled). For additional information, refer to *Disabling an Endpoint* on page 182. |
| **Manage Modules...** | Opens the ***Add/Remove Modules*** dialog, which lets you manage agent features for modules install on Lumension Endpoint Management and Security Suite. For additional information, refer to *Managing Endpoint Modules* on page 182. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br><br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |

## Endpoint Information

The fields that appear in the Endpoint Information section of the ***Information*** tab contain identifier and operating system details.

The **Endpoint Information** section displays the following device data:

Figure 65: Endpoint Information

Table 65: Endpoint Information Field Descriptions

| Field | Description |
|---|---|
| **Endpoint Name** | The name of the endpoint. |
| **DNS** | The DNS name of the endpoint. |
| **IP** | The IP Address of the endpoint. |
| **MAC Address** | The MAC address of the endpoints. |
| **Description** | The description of the endpoint, if available. |
| **Operating System** | The abbreviated name of the operating system detected on the endpoint. |
| **OS Version** | The version number of the operating system running on the endpoint. |
| **OS Service Pack** | The service pack level of the endpoint. |
| **OS Build Number** | The build number of the operating system running on the endpoint. |

## Agent Information

The fields that appear in the **Agent Information** section of the ***Information*** tab contain agent status, version, and connectivity details for the agent installed on the endpoint.

The **Agent Information** section displays the following agent data.

Table 66: Agent Information Field Descriptions

| Field | Description |
|---|---|
| **Agent Version** | The agent version number defined for the endpoint. |
| **Agent Installation Date** | The date the agent registered with Lumension Endpoint Management and Security Suite. This is typically the date the agent was installed on the endpoint. |

| Field | Description |
|---|---|
| **Uninstall Password** | Click **View** to view the uninstall password assigned to the endpoint. See *Viewing the Agent Uninstall Password* on page 180 for more information. |

### Status Information

The fields that appear in the **Status Information** section of the ***Information*** tab contain status and connectivity details for the agent installed on the endpoint.

The **Status Information** section displays the following agent data.

Table 67: Status Information Field Descriptions

| Field | Description |
|---|---|
| **Agent status** | The status of the agent (`Disabled`, `Offline`, `Online`, `Sleeping`, `Working`, or `Unknown`). This information is also shown on the ***Endpoints*** page. |
| **Last connected date** | The date the agent last communicated with Lumension Endpoint Management and Security Suite. |

### Component Information

This table lists information related to the module installs, licenses, and versions.

The following table describes each **Component Information** table column.

Table 68: Component Information Table

| Column | Description |
|---|---|
| **Component** | Indicates the name of the applicable module. |
| **Available with the Agent Version** | Indicates whether the module agent features are available for the installed agent version. |
| **Installed** | Indicates whether the module is installed on the endpoint. |
| **Installation Date/Time (Server)** | Indicates the date and time the module was installed, if applicable. |
| **Running Version** | Indicates the version of the module installed on the agent. |
| **Policy Version** | Indicates the version of the module that should be installed based on the agent version defined in the applicable agent policy set. |

### Group Information

The fields that appear in the **Group Information** section of the ***Information*** tab contain group membership details for the endpoint.

The **Group Information** section displays the following group data.

Table 69: Group Information Section Field Descriptions

| Field | Description |
|---|---|
| **Group Name** | Indicates the name or the IP address of the group(s) that the endpoint is a member of. Click the group name to go to the ***Group Information*** page. |
| **Originating Group** | Indicates the name or the IP address of the parent group that the endpoint is a member of. Click the originating group name to go to the ***Group Information*** page. |
| **Type** | Indicates the group type. This can be a system created groups (OS), directory service, or custom group. |
| **Deployments Applicable** | Indicates that there are applicable deployments available for this endpoint. |
| **Added By** | Indicates the Lumension Endpoint Management and Security Suite user who added the endpoint to the group. System created groups indicate `Lumension Corp.` in this field. |
| **Added On** | Indicates the date and time that the endpoint was added to the group. |

**Note:** If the values in the **Group Name** and the **Originating Group** fields are the same, then the endpoint is an actual (not inherited) member of that group. In addition, actual group members are shaded in white and appear at the top of the **Group Information** list. Groups that are shaded in gray are inherited.

### Policy Information

The fields that appear in the **Policy Information** section of the ***Information*** tab contain details about the policies used by the endpoint during a deployment.

These policies are the results of applying each of the policies defined by the endpoint's group membership and filling in any undefined policies from the Global Policy. Conflict resolution rules are applied when applicable.

Table 70: Policy Information Field Descriptions

| Name | Description |
|---|---|
| **Download via HTTP** | Indicates whether the agent downloads packages using HTTP, regardless of whether HTTPS is used for agent to server communication. |
| **Lumension EMSS agent version** | Indicates the version of the agent installer. |
| **Agent uninstall protection** | Indicates whether uninstall password protection for the agent is enabled. |
| **Maximum Transfer Rate** | Indicates the maximum bandwidth used when downloading packages to an agent. A value of *0* indicates bandwidth throttling is disabled. |

| Name | Description |
|---|---|
| **Minimum File Size** | Indicates the smallest file size which will be impacted by bandwidth throttling. |
| **Agent Scan Mode** | Defines the agents detection scan mode. A value of *0* mean *Slow*, a value of *1* means *Fast the first time*, and a value of *2* means *Fast*. |
| **Scheduling Frequency** | Indicates the number of hours between scheduled detection scans. |
| **Deployment: User May Cancel** | Indicates whether the user can cancel a deployment. A value of *Y* means yes, and a value of *N* means no. |
| **Deployment: Always on Top** | Indicates whether the PDDM will remain the topmost window. A value of *Y* means yes, and a value of *N* means no. |
| **Deployment: Deploy within** | Indicates the defined time window (in minutes) during which the user may snooze or cancel a deployment. |
| **Deployment: User May Snooze** | Indicates whether a user can cancel a deployment. A value of *Y* means yes, and a value of *N* means no. |
| **Resume Interrupted Downloads** | Indicates whether resumable downloads are enabled. A value of *0* means no, and a value of *1* means yes. |
| **Maximum Log File Size** | Indicates the endpoint service maximum log size (in MB). |
| **Logging Level** | Indicates the endpoint service logging security level. |
| **Agent Listener Port** | Defines the agent listener port. A value of *0* indicates agent listener is disabled. |
| **Reboot: User May Cancel** | Indicates whether the user can cancel a reboot. A value of *Y* means yes, and a value of *N* means no. |
| **Reboot: Reboot Within** | Indicates the defined time window (in minutes) during which the user may snooze or cancel a reboot. |
| **Reboot: User May Snooze** | Indicates whether the user can snooze a reboot. A value of *Y* means yes, and a value of *N* means no. |
| **Servers** | Indicates the available FastPath routes. |
| **Agent/Server Communication Protocol** | Indicates the protocol used in agent to server communications. |
| **Heartbeat Interval** | Indicates the endpoint service communication heartbeat interval (in minutes). |
| **Send Interval** | Indicates the endpoint service communication send delay interval (in seconds). |

| Name | Description |
|---|---|
| **Receive Interval** | Indicates the endpoint service communication receive delay interval (in seconds). |
| **Timeout Interval** | Indicates the endpoint service communication receive timeout interval (in seconds). |
| **Fast Path Interval** | Indicates the interval (configurable in minutes, hours, and days) between each check by FastPath to determine the fastest communication path back to the server. A value of *0* indicates that FastPath is disabled and a value of *1* indicates that FastPath is enabled. |
| **Communication Interval** | Indicates the time period between agent communication attempts (refer to IntervalType for the time period definition). |
| **Hours of Operation: Monday** | Defines the agent Hours of Operation (HOP) for Monday |
| **Hours of Operation: Tuesday** | Defines the agent Hours of Operation (HOP) for Tuesday |
| **Hours of Operation: Wednesday** | Defines the agent Hours of Operation (HOP) for Wednesday |
| **Hours of Operation: Thursday** | Defines the agent Hours of Operation (HOP) for Thursdays |
| **Hours of Operation: Friday** | Defines the agent Hours of Operation (HOP) for Friday |
| **Hours of Operation: Saturday** | Defines the agent Hours of Operation (HOP) for Saturday |
| **Hours of Operation: Sunday** | Defines the agent Hours of Operation (HOP) for Sunday |
| **InventoryCollectionsOptions: BIOS** | Indicates whether BIOS data will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: CPU** | Indicates whether CPU data will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: Custom** | Indicates whether custom inventory data will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: DISK_DRIVES** | Indicates whether data regarding the disk drives will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: ENABLE_WMI** | Indicates whether WMI data will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |

| Name | Description |
|---|---|
| **InventoryCollectionsOptions: HW_DEV_OTHER** | Indicates whether the Windows registry will be scanned for additional hardware information during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: HW_IDE_CONTROL** | Indicates whether data regarding IDE ATA/ATAPI controllers will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: HW_NETWORK_AD...** | Indicates whether data regarding network adapters will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: HW_NON_PNP** | Indicates whether data regarding non-Plug and Play drivers will be be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: HW_SND_GAME** | Indicates whether data regarding sound, video, and game controllers will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: HW_SYS_DEV** | Indicates whether system device data will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: HW_USB** | Indicates whether data regarding USB device inventory (from Enum \USB) will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: HW_USB_CONTROL** | Indicates whether data regarding USB controllers will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: HW_USB_STORAGE** | Indicates whether data regarding USB device inventory (from ENUM \UBSTOR) will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: LAST_REBOOT** | Requires **InventoryCollectionsOptions: ENABLE_WMI** value to be set to *ON*. Indicates whether the last reboot time gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: LAST_USER** | Indicates whether the last logged in user and time will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: MANUF_MODEL** | Requires **InventoryCollectionsOptions: ENABLE_WMI** value to be set to *ON*. Indicates whether the computer manaufacturer and model will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |

| Name | Description |
|---|---|
| **InventoryCollectionsOptions: None** | **InventoryCollectionsOptions:None**. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: OS_SERIAL** | Requires **InventoryCollectionsOptions: ENABLE_WMI** value be set to *ON*. Indicates whether the OS serial number will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: PC_ASSET_TAG** | Requires **InventoryCollectionsOptions: ENABLE_WMI** value be set to *ON*. Indicates whether the devices asset tag will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: PC_SERIAL** | Requires **InventoryCollectionsOptions: ENABLE_WMI** value be set to *ON*. Indicates whether the devices serial number will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: RAM** | Indicates whether the devices total RAM will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: SERVICES** | Indicates whether a listing of Windows services (not applicable for Windows 9x or ME) will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: SOFTWARE** | Indicates whether a listing of installed software will be gathered during agent inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |
| **InventoryCollectionsOptions: VIRTUAL** | Indicates whether the devices virtualization status will be gathered during inventory collection. A value of *ON* means the data will be collected and *OFF* means it will not. |

## Working with the Endpoint Details Page

You can perform a number of tasks related to endpoints from the ***Endpoint Details*** page. You perform most of these tasks regardless of the tab selected. However, certain tasks are specific to certain tabs.

To perform mosts tasks associated with endpoints, click a toobar button. To perform some tasks, selecting one or multiple endpoints from the page list may be necessary.

The following list displays the tasks you can perform from the ***Endpoint Details*** page, followed by the tabs that you perform them from.

- *Viewing the Agent Uninstall Password* on page 180 (***Information*** tab)
- *Defining the Endpoint Agent Version (Endpoint Details)* on page 181 (***Information*** tab)
- *Enabling an Endpoint* on page 181 (***Information*** tab)
- *Disabling an Endpoint* on page 182 (***Information*** tab)
- *Managing Endpoint Modules* on page 182 (***Information*** tab)
- *Managing Endpoint Modules* on page 182 (***Information*** tab)
- *Exporting Endpoint Information* on page 170 (all ***Endpoint Details*** page tabs)

## Viewing the Agent Uninstall Password

The uninstall password for an endpoint is required to remove the agent locally from the endpoint. You should make note of this password before attempting to uninstall an agent.

1. Select **Manage** > **Endpoints**.

   **Step Result:** The ***Endpoints*** page displays.

2. Click the link in the **Name** column that corresponds to the endpoint for which you want to uninstall the agent password for.

   **Step Result:** The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.

3. Click **View...**.

   **Step Result:** ***Agent Uninstall Password*** dialog displays.

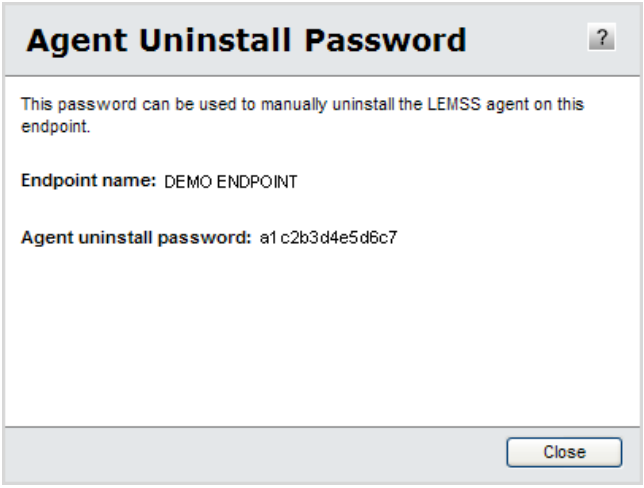

Agent Uninstall Password
?
This password can be used to manually uninstall the LEMSS agent on this endpoint.
Endpoint name: DEMO ENDPOINT
Agent uninstall password: a1c2b3d4e5d6c7
Close

Figure 66: Agent Uninstall Password Dialog

4. Click **Close** to close the ***Agent Uninstall Password*** dialog.

### The Agent Uninstall Password Dialog

The Agent Uninstall Password dialog contains the endpoint's name and the password that is required to uninstall the agent locally from an endpoint.

The following table describes the fields that appear on the ***Agent Uninstall Password*** dialog.

Table 71: Agent Uninstall Password Dialog Fields

| Field | Description |
|---|---|
| **Endpoint name** | The endpoint's name. |
| **Agent uninstall password** | The password required to uninstall the agent from the endpoint locally. |

## Defining the Endpoint Agent Version (Endpoint Details)

From the ***Endpoint Details*** page, you define which version(s) of the Lumension Endpoint Management and Security Suite Agent can be installed on the endpoint.

Define agent version(s) for the endpoint from the endpoints from ***Information*** tab.

1. Select **Manage** > **Endpoints**

   **Step Result:** The ***Endpoints*** page opens to the ***All*** tab.

2. Click the link associated with endpoint you want to define agent version(s) for.

   **Step Result:** The ***Endpoint Details*** page for the endpoint opens to the ***Information*** tab.

3. Click **Agent Versions...**.

   **Step Result:** The ***Manage Agent Versions*** dialog opens.

4. Select an agent version from the **Agent Version** list.

   **Note:** The agent versions available for selections are defined from the ***Options*** page. For additional information, refer to *Configuring the Agents Tab* on page 80.

5. Click **OK**

**Result:** The ***Manage Agent Versions*** dialog closes. If an agent version other than the defined version is installed on the endpoints, the defined version is installed over the previous version.

## Enabling an Endpoint

Enabling an endpoint includes the endpoint in the content management activities of the Lumension Endpoint Management and Security Suite.

You can enable an endpoint from the ***Endpoint Details*** page.

1. Select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint that you want to enable.

   **Step Result:** The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.

3. Click **Enable**.

**Result:** The endpoint is enabled.

## Disabling an Endpoint

Once disabled, modules installed on the endpoint no longer function.

You can disable an endpoint from the ***Details for Endpoint*** page.

1. Select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds with the endpoint you want to disable.

   **Step Result:** The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.

3. Click **Disable**.

   **Step Result:** A ***disable confirmation*** dialog displays.

4. In the ***confirmation*** dialog box, click **OK**.

**Result:** The endpoint is disabled. After disabling an agent, the endpoint can be deleted from Lumension Endpoint Management and Security Suite.

> **Note:** Once disabled, the endpoint may not appear in the ***Endpoints*** page list based on the **Status** filter settings. To include disabled devices in the list, ensure you select **Disabled** or **All** in the **Status** filter.

## Managing Endpoint Modules

You may select which modules licenses an endpoint's agent uses. Using this feature allows you control which modules apply to a particular endpoint.

Manage modules for individual endpoints from the ***Add/Remove Modules*** dialog.

1. Select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint for which you want to manage endpoint modules.

   **Step Result:** The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.

3. Click **Manage Modules...**.

   **Step Result:** The ***Add/Remove Modules*** dialog opens.

4. Manage modules for each endpoint.
   - To add a module to a particular endpoint, select the module checkbox for the applicable endpoint.
   - To remove a module from a particular endpoint, clear the module checkbox for the applicable endpoint.

> **Tip:** Select or clear the **Select All** check box(es) associated with a module to globally toggle a module for all endpoints.

5. Click **OK**.

**Result:** The ***Add/Remove Modules*** dialog closes. The agent features for each edit are updated during the next Discover Applicable Updates task.

## Exporting Endpoint Information

You can export the endpoint information generated in the Lumension Endpoint Management and Security Suite so that it can be used in other applications.

The export utility lets you export endpoint information to a comma-separated value (`.CSV`) file format. For additional information, refer to *Exporting Data* on page 37.

# Chapter 8

# Using Groups

**In this chapter:**


- About Groups
- The Groups Page
- The Information View
- The Group Membership View
- The Endpoint Membership View
- The Agent Policy Sets View
- The Roles View
- The Dashboard View
- The Settings View


Groups are collections of endpoints. By organizing endpoints into a group, you can manage them collectively rather than individually.

You can organize groups using any desired criteria. Some examples are:

- Operating System
- Endpoint Function
- Organization Divisions
- User Roles

Use of groups reduces individual endpoint maintenance.

## About Groups

A *group* is a collection of endpoints that lets you manage endpoints collectively for security management purposes.

Lumension Endpoint Management and Security Suite (Lumension EMSS) contains the following group types:

- Predefined System Groups
- Custom Groups

For additional information about group types, refer to *Defining Groups* on page 188.

Within Lumension EMSS, you can nest groups; groups can contain other groups. These related groups, called parent and child groups, minimize Lumension EMSS maintenance.

# The Groups Page

Use this page to control groups. The functions from many other Lumension Endpoint Management and Security Suite (Lumension EMSS) pages are available from this page (the ***Endpoints*** page, the ***Users and Roles*** page, and so on). However, the functions performed on the ***Groups*** page pertain primarily to the selected group's endpoints.

Groups are selected from the **Group Browser**, a ***Groups*** page pane. The browser displays an expandable directory tree that lists parent and child groups. From this browser, you can access group information by clicking a group. Information for the selected group displays in the main pane.

To view the ***Groups*** page, select **Manage** > **Groups**.

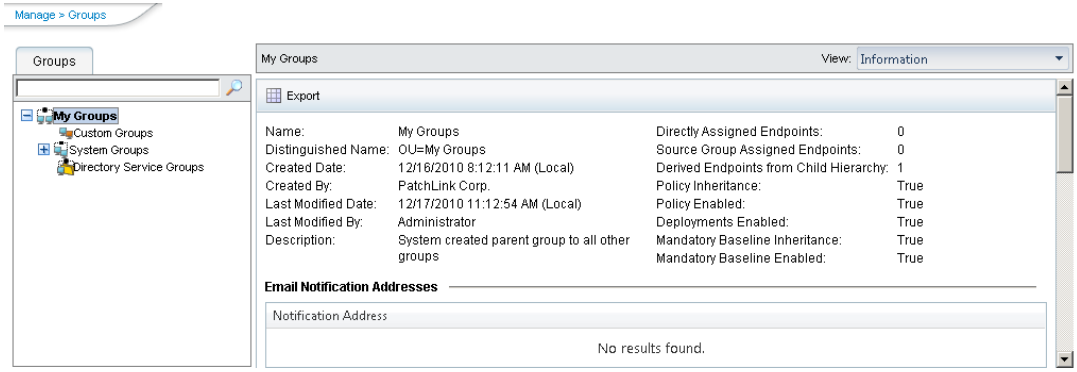



Figure 67: Groups Page

Unlike most other Lumension EMSS pages, which are organized by tabs, the ***Groups*** page is organized by views, which are selectable from the **View** list. The information displayed for a selected group changes according to view.

The views are:

- *The Information View* on page 189
- *The Group Membership View* on page 194
- *The Endpoint Membership View* on page 200
- *The Agent Policy Sets View* on page 207
- *The Roles View* on page 211
- *The Dashboard View* on page 215
- *The Settings View* on page 218

## The Group Browser Directory Tree

Use the **Group Browser**, a ***Groups*** page pane, to select a group. The number of groups in the tree depends on the number of groups created.

Click an **Expand** icon (+) to view custom, system, and directory service groups. By continuing to expand the tree, you can view parent groups and their nested child groups.

To display detailed group information, select a group name.

After selecting a group, use the **View** list to access different views, such as the ***Information*** view or the ***Group Membership*** view.

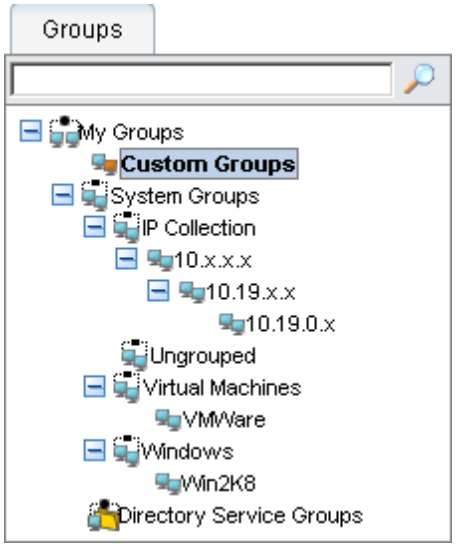



Figure 68: Group Browser Directory Tree

## Parent and Child Groups

Within the **Group Browser** directory tree, groups are nested in hierarchical relationships. This hierarchy contains *parent* groups and *child* groups. These terms are used to describe groups (parent groups) that contains any number of nested groups (child groups). Each group has only one parent. However, a parent group can have multiple child groups. Nesting child groups within parent groups creates an inheritance, which lets you apply one agent policy set to a parent and its descendants.

Parent-child relationships creates the following hierarchies within groups:

| | |
|---|---|
| **Group Hierarchy** | Refers to the entire group hierarchy from the original to the deepest child group. |
| **Parent Hierarchy** | Refers to the entire group hierarchy above a specific group. |
| **Child Hierarchy** | Refers to the entire subordinate group hierarchy below a specific group. |
| **Inheritance** | Refers to the permissions a group has set. Group inheritance settings must have a value of `True` to inherit its parent settings. |

**Note:** System and directory service group hierarchies cannot be modified.

### Defining Groups

Within Lumension Endpoint Management and Security Suite (Lumension EMSS), there are several types of groups. Some groups are created by users, while others are created by the Lumension EMSS system. When working with groups, only user-created groups can be deleted.

Groups are categorized into the following classifications.

Table 72: Group Definitions

| Icon | Group Type | Definition |
|---|---|---|
| | Parent System Groups | Endpoints identified in your network are automatically assigned a group membership based on their operating system, Active Directory (AD) membership, or IP address. However, you can also manually define an endpoint's initial custom group assignment when creating an agent management job. Not all operating systems, AD groups, or IP ranges may be shown. This omission is because Lumension EMSS creates system groups based on only the endpoints present in your network. Groups are also created for virtual machines (the **Virtual Machines** group) and managed endpoints that have not yet been added to a custom group (the **Ungrouped** group). You cannot modify system groups or their hierarchies.<br>**Note:** Within IP groups, only agent version 6.4 or later appear. |
| | System Groups | |
| | Parent Directory Service Groups | Created when an agent submits a directory service hierarchy that does not already exist in Lumension EMSS. You cannot modify directory service groups or their hierarchies. |
| | Directory Service Groups | |
| | Custom Groups (Parent & Child) | Custom groups are created and managed by the user. |

## Viewing Groups

Navigate to the ***Groups*** page to work with groups. After navigating to the page, select a group and a view.

You can select this page from the navigation menu at any time.

1. Select **Manage** > **Groups**.
2. Expand the **Group Browser** directory tree to the desired group.
3. Select the group.

   **Step Result:** The selected group's information displays.

4. Select the desired view from the **View** list.

**Result:** The selected group's information displays on the main portion of the screen. Select a different view from the **View** list to change the information displayed.

### Searching for a Group

The **Group Browser** contains a field you can use to search for groups. Use this field in network environments containing many groups. After entering search criteria, the browser directory tree changes to a listing of groups specified in the field.

This field uses a *contains* search condition. Wildcards are not supported.

1. Select **Manage** > **Groups**.

   **Step Result:** The ***Groups*** page opens.

2. In the **Group Browser** field, type your search criteria.

   **Step Result:** The results for your search displays below the **Group Browser** field as you type.

3. Click the desired group.

**Result:** Information for the selected group displays on the ***Groups*** page. Click the ***Group Browser*** **delete** icon to return to the directory tree.

## The Information View

This view includes basic information about the selected group's membership, hierarchy, agent policy sets, roles, and so on. Select this view for a comprehensive listing of the selected group's settings.

Group settings and information appear in sections. Each section displays information for each type of group settings. Empty sections indicate undefined settings.

The ***Information*** view features the following informational tables:


- *Information View* on page 190
- *Email Notification Addresses* on page 191
- *Child Groups* on page 191
- *Agent Policy Sets* on page 192
- *Resultant Agent Policy Set Information* on page 192
- *Roles* on page 193
- *Exporting Information View Data* on page 193

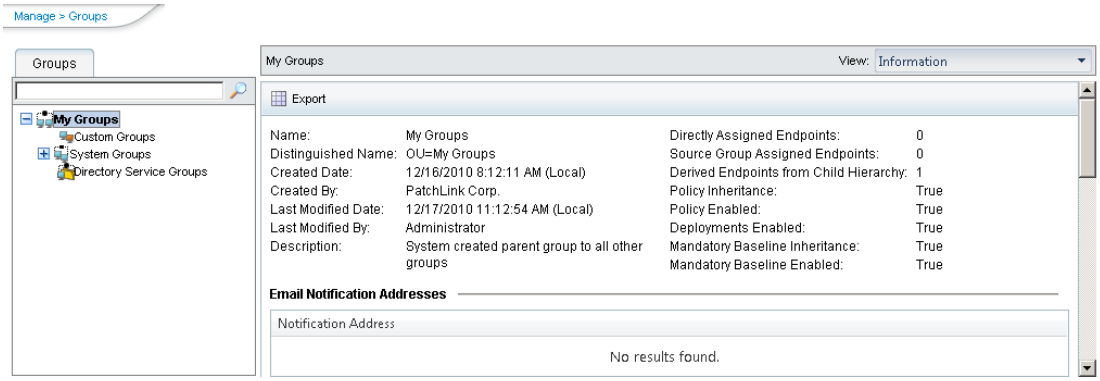




Figure 69: Group Information

The following table describes the ***Information*** view buttons.

Table 73: Information View Button

| Button | Function |
|---|---|
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br><br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |

## Information View

This view displays general information about the selected group's settings. These settings are controlled within the various ***Groups*** page views. Select this view when you want to see a group's settings from a single source.

The following table describes the **Information** view fields.

Table 74: Group Information

| Field | Description |
|---|---|
| **Name** | Indicates the name of the group. |
| **Distinguished Name** | Indicates the system-created name based upon the group’s parent hierarchy. |

| Field | Description |
|---|---|
| **Created Date** | Indicates the date and time the group was created. |
| **Created By** | Indicates the user who created the group. |
| **Last Modified Date** | Indicates the date and time the group was last modified. |
| **Last Modified By** | Indicates the user who last modified the group. |
| **Description** | Indicates the description of the group. |
| **Directly Assigned Endpoints** | Indicates the number of endpoints assigned to the group. Inherited endpoints are not included. |
| **Source Group Assigned Endpoints** | Indicates the number of endpoints assigned to the source group. |
| **Derived Endpoints from Child Hierarchy** | Indicates the number of endpoints inherited from child groups. |
| **Policy Inheritance** | Indicates if agent policy sets are inherited from the group's parent (`True` or `False`). |
| **Policy Enabled** | Indicates if agent policy sets can be assigned to the group (`True` or `False`). |

## Email Notification Addresses

After a group is created, it can be assigned an email address. This email is intended to be attributed to the group's owner, which is the user that created the group. Email addresses are not assigned via the ***Information*** view; this view merely displays the assigned addresses. Addresses are assigned via the ***Settings*** view.

The following reference describes the **Email Notification Addresses** table.

Table 75: Email Notification Addresses Table

| Column | Description |
|---|---|
| **Notification Address** | The email addresses of the group owner. |

## Child Groups

This section lists the selected group's direct child groups. Only direct children are listed; deeper descendants such as grandchild groups are not listed. Assign child groups to the selected group via the ***Group Membership*** view.

The following reference describes each table column.

Table 76: Child Groups Table

| Column | Description |
|---|---|
| **Type** | The group type (`Custom Group`, `System Group`, or `Directory Service Group`). |

| Column | Description |
|---|---|
| **Group Name** | The name of the child group. |
| **Distinguished Name** | The system-created name of the group, which is based upon the group's parent hierarchy. |
| **Group Description** | The description of the group. |

## Agent Policy Sets

This section lists the agent policy sets assigned to the selected group, and whether or not that policy set is directly assigned or assigned via inheritance. This section only lists assigned policy sets; you cannot use it to assign them. Assign policy sets to the selected group via the ***Policies*** view.

The following reference describes the **Policy Sets** table.

Table 77: Policy Sets

| Field | Description |
|---|---|
| **Policy Set Name** | Indicates the name of the agent policy set. |
| **Assigned** | Indicates if the agent policy set is directly assigned to the group or inherited. A value of `True` indicates the agent policy set is directly assigned. |

**Note:** When a group's **Policy Enabled** setting is enabled, the group will uses the global system policy set to define undefined policies. For additional information, refer to *Defining Agent Policy Inheritance Rules* on page 232.

## Resultant Agent Policy Set Information

When a group is assigned two or more agent policy sets, some of the policy settings may conflict. By applying the agent policy conflict resolution rules, the system determines which policy settings to apply. This section lists the resultant policy settings used when agent policy sets conflict. Scroll down if necessary to view all resultant policy settings.

The following reference describes the ***Resultant Agent Policy Set Information*** table.

Table 78: Resultant Agent Policy Set Information

| Field | Description |
|---|---|
| **Name** | The name of the agent policy. |
| **Value** | The agent policy value. When determining the policy value, directly assigned policies supersede inherited policies. Additionally, directly assigned policies that conflict are resolved by the conflict resolution rules. |

| Field | Description |
|---|---|
| **Description** | The description of the agent policy. |

**Note:** Only agent policies inherited or directly assigned to the group are displayed in **Resultant Agent Policy Set Information**. To see a complete listing of all policies assigned to a managed endpoint, refer to *The Information Tab* on page 172.

## Roles

Within Lumension Endpoint Management and Security Suite, you can restrict user access to specific groups based on roles. This section lists the user roles that can access the selected group. This section merely lists the roles that can access the group; you cannot use it to assign roles to the group. To define roles that access the group, edit the accessible groups when creating or editing a role.

The following reference describes the **Roles** table.

Table 79: Roles

| Field | Description |
|---|---|
| **Role Name** | Indicates the name of the user role that can access the group. |
| **Role Source** | Indicates the name of the group that the assigned role is inherited from. If the role source contains no value, the role is directly assigned to the selected group. |
| **Assigned** | Indicates if the role is inherited or directly assigned to the group. A value of `True` indicates the role is directly assigned to the group. |

## Exporting Information View Data

To export the information displayed within the ***Information*** view to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to *Exporting Data* on page 37.

# The Group Membership View

This view lets you view the selected group's direct child groups. If the selected group is a custom group, you can also create new custom child groups that you can populate with the desired endpoints. Custom groups also let you edit or delete any listed, preexisting child groups.

This view only lists direct child groups; you cannot manage grandchild groups or further descendants.

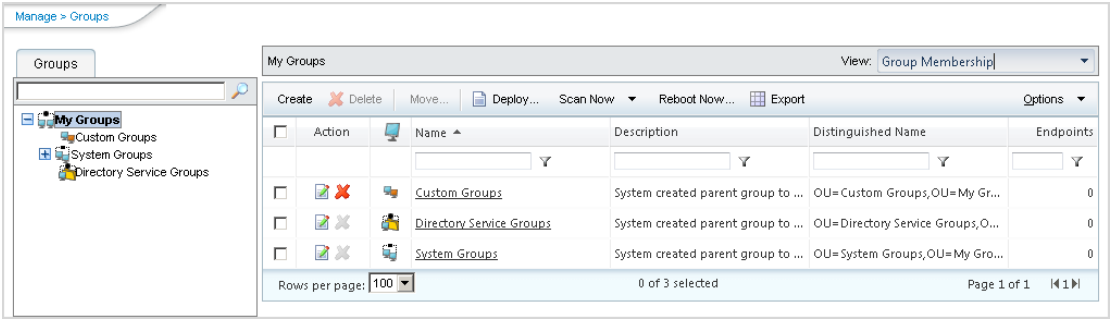



Figure 70: Group Membership View

## The Group Membership View Toolbar

This toolbar contains buttons related to the creation and management of groups. It also lets you deploy content, as well as scan and reboot endpoints.

The following table describes the toolbar functions. Some functions are common to all the ***Groups*** page views.

Table 80: Group Membership Toolbar

| Button | Function |
|---|---|
| **Create** | Creates a new group. For additional information, refer to *Creating a Group* on page 195. |
| **Delete** | Deletes a group. For additional information, refer to *Deleting Groups* on page 197. |
| **Move...** | Assigns a group to a new parent group. For additional information, refer to *Moving a Group* on page 197. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |
| **Options** (menu) | Opens the **Options** menu. For additional information, refer to *The Options Menu* on page 31. |

## The Group Membership View List

This list displays the selected group's direct child groups. Each listing contains group identification information and icons used to edit identification information or delete the group altogether.

The following table displays the ***Group Membership*** view list details.

Table 81: Group Membership View

| Column | Icon | Description |
|---|---|---|
| **Action** | | Contains **Edit** and **Delete** icons. Use these icons to edit or delete the associated group. |
| **Groups** | | Contains an icon that indicates the group type (system or custom). |
| **Name** | | Indicates the name of the child group. |
| **Description** | | Indicates the description of the group. |
| **Distinguished Name** | | Indicates the system-created name based upon the group's parent hierarchy. |
| **Endpoints** | | Indicates the number of endpoints assigned to the group. |

**Note:** ***System*** and ***Directory Service*** groups cannot have their child group or endpoint memberships edited. However, their assigned agent policy sets can be edited.

## Creating a Group

Lumension Endpoint Management and Security Suite provides preconfigured groups. However, you can also create custom groups. Populate custom groups with desired endpoints. You can only create custom groups within the **Group Browser** custom group hierarchy.

Create groups from the ***Group Membership*** view.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. Select the ***Custom Group*** from the directory tree that you want to create a child group for.

4. Click **Create**.

   **Step Result:** A new row appears on the page.

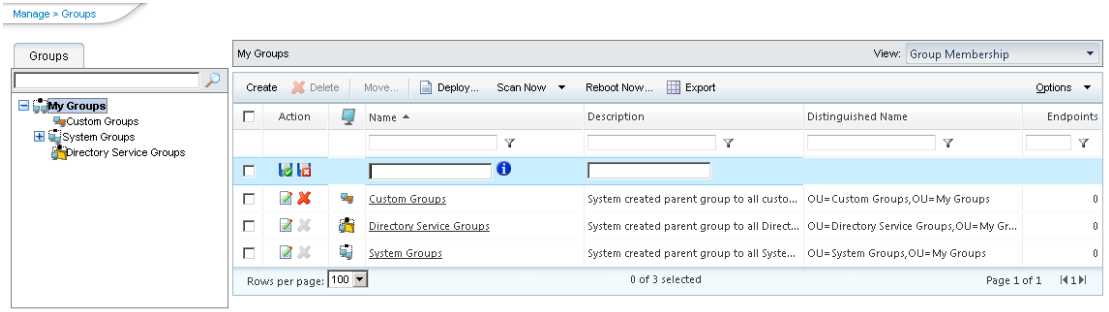



Figure 71: New Row

5. In the **Name** field, type a name for the group.
6. If desired, type a brief description about the group in the **Description** field.
7. Click the **Save** icon associated with the new group.

**Result:** The group is saved to the list and is added to the directory tree. A ***Distinguished Name*** is generated for the group.

**After Completing This Task:**

Add endpoints to the group. For additional information, refer to *Adding Endpoint Members* on page 202.

## Editing Groups

If desired, you can edit the names and descriptions for custom groups. In the ***Group Membership*** view, you can only edit group names and descriptions, not their settings.

You can only edit the names for groups within the **Custom Groups** hierarchy. Edit groups from the ***Group Membership*** view.

**Note:** The **My Groups** group **Name** and **Description** cannot be edited. Additionally, within the **System Groups** and **Directory Service Groups** hierarchies, only group **Descriptions** can be edited, not their **Names**.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. From the directory tree, select the parent group of the group you want to edit.
4. Click the **Edit** icon associated with the group you want to edit.
5. If desired, edit the **Name** field associated with the group.
6. If desired, edit the **Description** field associated with the group.

7. Click the **Save** icon.

**Result:** The changes are saved to the group.

> **Note:** Within the ***Group Membership*** view, you can only edit the group name and description. To edit group behavior, use the ***Roles***, ***Policies***, ***Membership***, ***Settings***, or ***Mandatory Baseline*** view.

## Deleting Groups

Delete a group when you no longer need to edit its endpoints. Only custom groups can be deleted. After deleting a group, there is no way to recover it; you must recreate the group.

Delete custom groups from the ***Groups Membership*** view.

> **Note:** Deleting a group does not prevent an endpoint within that group from deploying or scanning; these tasks occur at the endpoint level.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. From the directory tree, select the parent group of the group(s) you want to delete.

> **Note:** Only groups within the **Custom Groups** hierarchy can be deleted.

4. Delete the desired group(s).
   Use one of the following methods.

| Method | Steps |
|---|---|
| **To delete a single group:** | Click the **Delete** icon associated with the group you want to delete. |
| **To delete multiple groups:** | 1. Select the check boxes associated with the groups you want to delete.<br>2. From the toolbar, click **Delete**. |

**Step Result:** A dialog appears asking you to acknowledge the deletion.

5. Acknowledge the deletion by clicking **OK**.

**Result:** The selected groups are deleted.

> **Caution:** When a group is deleted, its child hierarchy is deleted as well.

## Moving a Group

After creating a group, you can change its position within the **Group Browser** directory tree.

You can only move groups within the **Custom Groups** hierarchy.

> **Note:** When moving a group, if the group is configured to inherit agent policies, roles, or baseline settings (Patch and Remediation only), the group inherits those values from its new parent.

1. Select **Manage** > **Groups**.

2. From the **View** list, select **Group Membership**.
3. From the directory tree, select the parent group of the group you want to move.
4. Select the check box associated with the group you want to move.
5. Click **Move...**.

   **Step Result:** The ***Move Groups*** window opens.

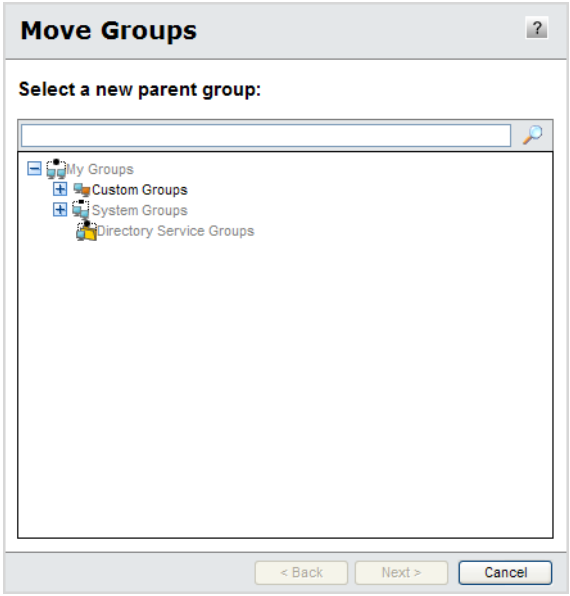



Figure 72: Move Groups Window

6. Select a new parent group.

7. Click **Next**.

   **Step Result:** The group is moved to the new parent group.

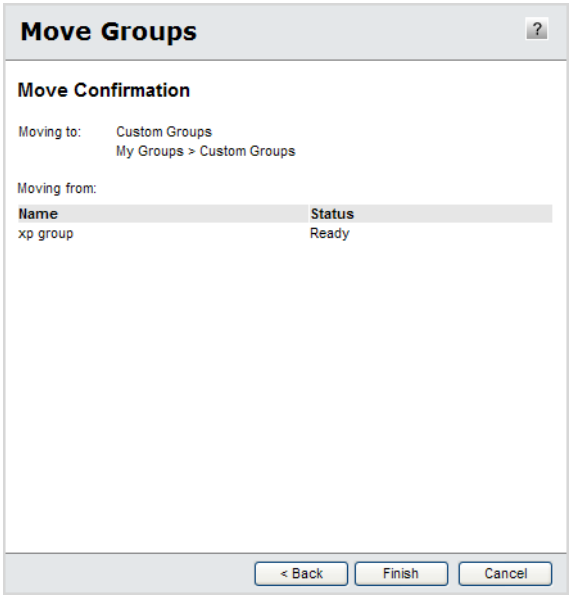



Figure 73: Move Confirmation

8. Click **Finish**.

## Exporting Group Membership View Data

To export information displayed in the ***Group Information*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to *Exporting Data* on page 37.

# The Endpoint Membership View

This view lists the endpoints that hold membership in the selected group. If the group selected is a custom group, you can also use this view to add endpoints. Use this view to manage endpoints assigned to the selected group. This view contains features similar to those available from the ***Endpoints*** page.

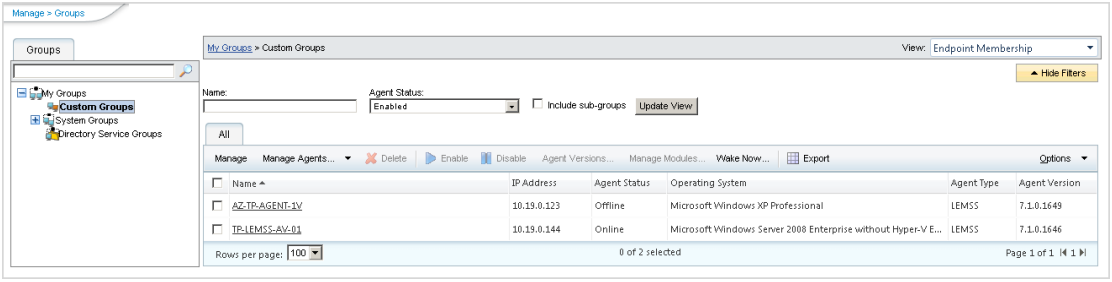



Figure 74: Endpoint Membership View

## The All Tab (Groups Page)

Use the ***All*** tab to perform tasks related to a selected group's endpoint. This tab is similar to the ***Endpoints*** page ***All*** tab, but lets you perform tasks from a group level.

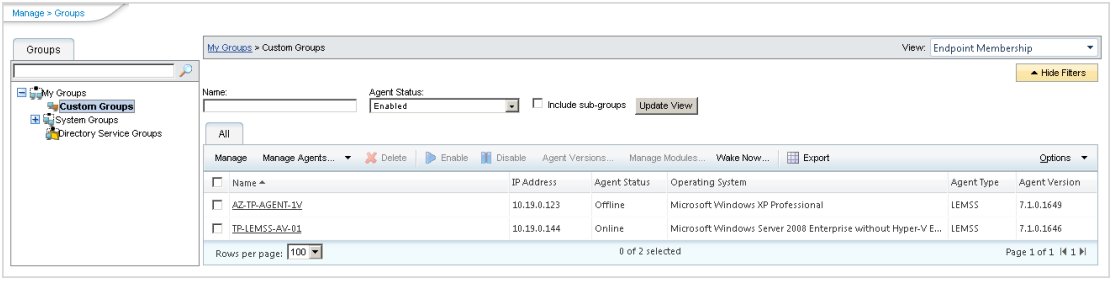



Figure 75: All Tab

### The All Tab Toolbar (Groups Page)

The ***All*** tab toolbar contains the tasks and functions that are available for you to perform for managed endpoints.

The following table describes the toolbar functions used in the ***All*** tab, available on the ***Groups*** page ***Endpoint Membership*** view.

Table 82: All Tab Toolbar (Groups Page)

| Button | Description |
|---|---|
| **Manage** | Adds or removes managed endpoints to or from the selected group. For additional information, refer to one of the following topics:<br>• *Adding Endpoint Members* on page 202<br>• *Removing Endpoint Members* on page 203 |

| Button | Description |
|---|---|
| **Manage Agents...** (menu) | Opens the Manage Agents menu. |
| **Install Agents...** (**Manage Agents...** menu item) | Installs agents on selected endpoints. For additional information, refer to *Installing Agents by Agent Management Job* on page 204. |
| **Uninstall Agents...** (**Manage Agents...** menu item) | Deletes agents from selected endpoints. For additional information, refer to *Uninstalling Agents by Agent Management Job* on page 204. |
| **Download Agent Installer...** (**Manage Agents...** menu item) | Downloads an agent installer to the endpoint used to access Lumension Endpoint Management and Security Suite. For additional information, refer to *Downloading the Agent Installer* on page 204. |
| **Agent Versions...** | Defines the agent version(s) that can be installed on an endpoint. For additional information, refer to *Defining the Endpoint Agent Version (Groups Page)* on page 205. |
| **Delete** | Deletes a disabled endpoint. For additional information, refer to *Deleting Endpoint (Groups Page)* on page 205. |
| **Enable** | Enables a disabled endpoint. For additional information, refer to *Enabling or Disabling Endpoints within a Group* on page 206. |
| **Disable** | Disables an enabled endpoint. For additional information, refer to *Enabling or Disabling Endpoints within a Group* on page 206. |
| **Manage Modules...** | Opens the Add/Remove Modules dialog. Use this dialog to toggle module-specific agent functions. For additional information, refer to *Managing Endpoint Modules (Groups Page)* on page 206. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |
| **Options** (menu) | Opens the **Options** menu. For additional information, refer to *The Options Menu* on page 31. |

### The All Tab List (Groups Page)

The ***All*** tab list itemizes endpoint operating system information, identification information, agent information, and module information.

The following table describes the columns within the ***All*** tab list.

Table 83: All Tab List Columns

| Column | Description |
|---|---|
| **Name** | Indicates the name of the endpoint. Clicking the ***Name*** link displays the applicable ***Endpoint Details*** page. See *The Endpoint Details Page* on page 171 for additional information. |
| **IP Address** | Indicates the IP address of the endpoint. |
| **Agent Status** | Indicates the status of the endpoint (`Online`, `Offline`, or `Disabled`). |
| **Operating System** | Indicates the operating system the endpoint is running. |
| **Agent Type** | Indicates the type of agent that is running on the endpoint and communicating with the Lumension Endpoint Management and Security Suite server. |
| **Agent Version** | Indicates the version number of the agent that is assigned to the endpoint. |
| ***Module*** **Installed** | Indicates whether a component module is installed on the endpoint. A ***Module*** **Installed** column appears for each component module installed on your Lumension Endpoint Management and Security Suite server. The following list defines column entry values:<br>**Yes** — The module is installed.<br>**Pending** — The module is pending install or uninstall.<br>**No** — The module is not installed.<br>**Error** — There was an error while installing or uninstalling the module. Click the error link for additional information about the error.<br>**Expired** — The module license has expired. |

## Adding Endpoint Members

Add endpoints to a group when those endpoints serve a similar function. Adding endpoints to a group lets you manage them collectively. You can only add endpoints to custom groups.

Add endpoints to a group from the ***Endpoint Membership*** view.

1. Select **Manage > Groups**.

2. From the **View** list, select **Endpoint Membership**.
3. Select a custom group from the directory tree.
4. Click **Manage**.

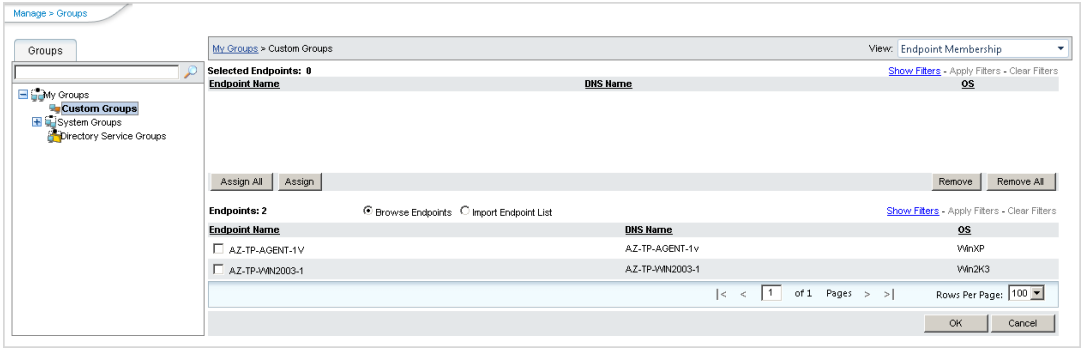



Figure 76: Manage Endpoints

5. Add endpoints to the group.
   Use one of the following methods.

| Method | Steps |
|---|---|
| **To add individual endpoints:** | 1. From the **Endpoints** list, select the check boxes associated with the endpoints you want to add to the group.<br>2. Click **Assign**. |
| **To add all endpoints:** | Click **Assign All**. |
| **To add endpoints through importation via a list:** | 1. Select the **Import Endpoint List** option.<br>2. If desired, select a group from the **Import endpoint list from existing group** list. Selecting a group from this list will automatically populate the field with applicable endpoint names.<br>3. Type the desired endpoint names in the field. Separate endpoint names with commas (,).<br>4. Click **Assign All**. |

**Step Result:** Endpoints are added to the **Selected Endpoints** table according to your input.

6. Click **OK**.

**Result:** The selected endpoints are added to the group. Click **Update View** to review the endpoint assignment.

## Removing Endpoint Members

When an endpoint no longer fits within the context of a group (for example, it no longer requires content applicable to the rest of the group), remove it from the group. You can re-add endpoints at any time.

Group endpoint removal takes place from the ***Endpoint Membership*** view.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. Select a custom group from the directory tree.
4. Click **Manage**.
5. Remove endpoints from the group.
   Use one of the following methods.

| Method | Steps |
|---|---|
| **To remove individual endpoints:** | 1. From the **Selected Devices** list, select the check boxes associated with the endpoints you want to remove from the group.<br>2. Click **Remove**. |
| **To remove all endpoints:** | Click **Remove All**. |

**Step Result:** Endpoints are removed from the **Selected Endpoints** table according to your input.

6. Click **OK**.

**Result:** The selected endpoints are removed from the group. Click **Update View** to review the endpoint assignment.

## Installing Agents by Agent Management Job

Within Lumension Endpoint Management and Security Suite, there are multiple methods of installing agents on endpoints using agent management jobs. To create an agent management job that installs agents from the ***Endpoint Membership*** view, select **Manage Agents...> Install Agents...** from the toolbar.

For additional information, refer to *Installing Agents by Agent Management Job* on page 111.

## Uninstalling Agents by Agent Management Job

Within Lumension Endpoint Management and Security Suite, there are multiple methods of uninstalling agents from endpoints using agent management jobs. To create an agent management job that uninstalls agents from the ***Endpoint Membership*** view, select **Manage Agents... > Uninstall Agents...** from the toolbar.

To prepopulate the ***Schedule Agent Management Job - Uninstall Wizard*** **target** list, first select the desired group from the **Group Browser Directory Tree**, and then select the check boxes associated with the desired endpoints.

For additional information, refer to *Installing Agents by Agent Management Job* on page 111.

## Downloading the Agent Installer

If you want to install an agent on the endpoint that you are currently using to access Lumension Endpoint Management and Security Suite, you can perform this task from the ***Endpoint Membership*** view.

To download an agent installer from the ***Endpoint Membership*** view, select **Manage Agents...> Download Agent Installer..** from the toolbar. For additional information, refer to *Downloading the Agent Installer* on page 166.

## Defining the Endpoint Agent Version (Groups Page)

From the ***Groups*** page, you can define which version(s) of the Lumension Endpoint Management and Security Suite Agent can be installed on group endpoints.

Define agent version(s) for group endpoints from the ***Groups*** page ***Endpoint Membership*** view.

1. Select **Manage** > **Groups** .

   **Step Result:** The ***Groups*** page opens.

2. From the **View** list, select **Endpoint Membership**
3. From the **Group Browser** directory tree, select the group containing endpoints for which you want to define agent version(s).
4. Select the endpoints on which you want to define agent version(s).
5. Click **Agent Versions...**.

   **Step Result:** The ***Manage Agent Versions*** dialog opens.

6. Define the agent version(s).

   Use one of the following methods:

| Method | Steps |
|---|---|
| **To define a standard agent version for all listed endpoints:** | • From the **Select One** list, select an agent version.<br>• Click **Apply to All Agents**. |
| **To define an agent version for each endpoint:** | Select an agent version from the **Agent Version** list for each endpoint. |

**Note:** The agent versions available for selections are defined from the ***Options*** page. For additional information, refer to *Configuring the Agents Tab* on page 80.

7. Click **OK**.

**Result:** The ***Manage Agent Versions*** dialog closes. If an agent version other than the defined version is installed on the endpoints, the defined version is installed over the previous version.

## Deleting Endpoint (Groups Page)

You can delete the list item for an endpoint.

Delete endpoint listing from the ***Endpoint Membership*** view.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. Select a custom group from the directory tree.
4. Select the endpoint listings you want to delete.

5. Click **Delete**.

   **Step Result:** A confirmation dialog opens.

6. Click **OK** to confirm the deletion.

**Result:** The list item for the selected endpoints are deleted.

## Enabling or Disabling Endpoints within a Group

Disabling an endpoint effectively deactivates its agent functionality. Disabled endpoints do not contact the Lumension Endpoint Management and Security Suite (Lumension EMSS) server, use Lumension EMSS features, or occupy Lumension EMSS licenses. Disable an endpoint if you want to prevent it from receiving a deployment in progress or if it will be unused for a prolonged period. You can re-enable an endpoint at any time.

Disable an endpoint within a group from the ***Endpoint Membership*** view.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. Select a group from the directory tree.
4. If necessary, define filter criteria and click **Update View**.
5. Select the check box(es) associated with the endpoint(s) you want to enable or disable.
6. Enable or disable the selected endpoint(s):
   Use one of the following methods.

| Method | Steps |
|---|---|
| **To enable a disabled endpoint:** | Click **Enable**. |
| **To disable an enabled endpoint:** | 1. Click **Disable**.<br>2. Acknowledge the disablement by clicking **OK**. |

**Result:** The applicable endpoints are enabled or disabled. The ***Endpoint Membership*** view and ***Endpoints*** page reflect your changes.

**Note:** Disabling an endpoint within a group is not limited to the group; the endpoint is completely disabled within the Lumension EMSS system.

## Managing Endpoint Modules (Groups Page)

You can manage endpoint module licences from the ***Groups*** page. Using this feature allows you control which modules apply to a particular endpoint.

Manage modules for individual endpoints from the ***Groups*** page ***Endpoint Membership*** view.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. From the directory tree, select the group containing endpoints you want to scan.
4. Select the checkbox(es) associated with the endpoints for which you want to manage modules.

5. Click **Manage Modules...**.

   **Step Result:** The ***Add/Remove Modules*** dialog opens.

6. Manage modules for each endpoint.

   - To activate a module for a particular endpoint, select the module checkbox for the applicable endpoint.
   - To deactivate a module for a particular endpoint, clear the module checkbox for the applicable endpoint.

   **Tip:** Select or clear the **Select All** check box(es) associated with a module to globally toggle a module for all endpoints.

7. Click **OK**.

**Result:** The ***Add/Remove Modules*** dialog closes. The agent features for each edit are updated during the next Discover Applicable Updates task.

### Exporting Endpoint Membership View Data

To export information displayed in the ***Endpoint Membership*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to *Exporting Data* on page 37.

## The Agent Policy Sets View

After creating agent policy sets, you can apply them to a group using the ***Agent Policy Sets*** view. From this view you can add or remove existing agent policy sets to or from the selected group. Additionally, you can create policy sets from this view. However, this view, unlike the ***Agent Policy Sets*** page, does not let you edit policy sets or view their details. This view is only applicable to agent policy sets.

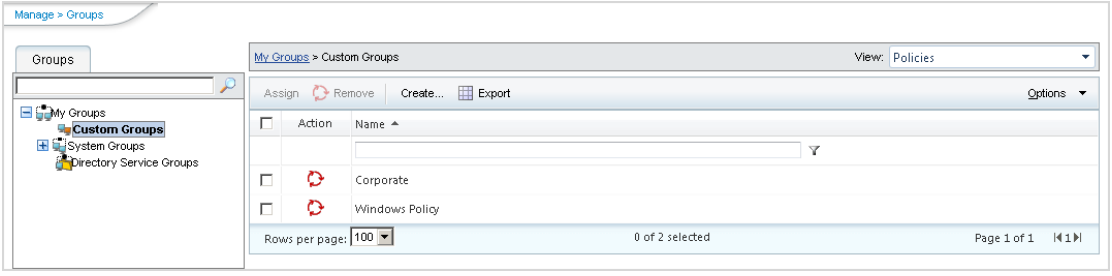



Figure 77: Agent Policy Set View

## The Agent Policy Sets View Toolbar

This toolbar contains buttons that let you manage agent policy sets in relation to groups. You can also create agent policy sets from this toolbar. Policy sets created from this toolbar can be applied to any group, not just the selected group.

The following table describes the ***Agent Policy Sets*** view toolbar.

Table 84: Agent Policy Sets View Toolbar

| Button | Function |
|---|---|
| **Assign** | Assigns an agent policy set to the selected group and its child groups. For additional information, refer to *Assigning an Agent Policy Set to a Group* on page 209. |
| **Remove** | Removes a selected agent policy set from the group. For additional information, refer to *Removing an Agent Policy Set from a Group* on page 209. |
| **Create...** | Creates an agent policy set. For additional information, refer to *Creating an Agent Policy Set (Groups Page)* on page 210. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |
| **Options** (menu) | Opens the **Options** menu. For additional information, refer to *The Options Menu* on page 31. |

## The Agent Policy Sets View List

This list itemizes all agent policy sets and policy details assigned to the selected group.

View the ***Agent Policy Sets View*** list from the ***Groups*** page. The following table describes each ***Agent Policy Sets View*** list.

| Column | Description |
|---|---|
| **Action** | Contains **Edit** and **Delete** icons. Use these icons to edit and delete the associated agent policy set. For additional information, refer to the following topics:<br>• *Editing an Agent Policy Set* on page 227<br>• *Deleting an Agent Policy Set* on page 228<br>**Note:** The **Global System Policy** cannot be deleted. |
| **Name** | The name of the agent policy set. |

## Assigning an Agent Policy Set to a Group

Associating an agent policy set with a group defines functional rules for the group to follow. Groups that do not have an associated agent policy set use the **Global System Policy**.

**Prerequisites:**

Create an agent policy set.

Assign agent policy sets to a group from the ***Agent Policy Set*** view.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Set**.
3. Select a group from the directory tree.
4. Click **Assign**.
5. Select an agent policy set from the **Select a Policy Set** list.
6. Click the **Save** icon.

**Result:** The policy set is saved and associated with the group.

## Removing an Agent Policy Set from a Group

When desired, you can remove an agent policy set from a group. Groups without associated policy sets use the global system policy to define their behavior.

Remove agent policy sets from a group from the ***Agent Policy Sets*** view.

**Note:** You cannot remove inherited policy sets. Instead, you must change the group's policy inheritance setting or remove the inherited policy set from the parent group.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Sets**.
3. Select a group from the directory tree.
4. Remove the desired policy sets.
   Use one of the following methods.

| Method | Steps |
|---|---|
| **To remove one agent policy set:** | Click the **Remove** icon associated with the policy set you want to remove. |
| **To remove multiple agent policy sets:** | 1. Select the check boxes associated with the agent policy sets you want to remove.<br>2. From the toolbar, click **Remove**. |

**Step Result:** A dialog appears, asking you to acknowledge the removal.

5. Acknowledge the removal by clicking **OK**.

**Result:** The agent policy set is no longer associated with the group and is removed from the ***Agent Policy Set*** view.

## Creating an Agent Policy Set (Groups Page)

You can create agent policy sets from the ***Agent Policy Set*** view. Agent policy sets are collections of values that can be assigned to groups to regulate how agents behave.

**Note:** When creating an agent policy set from the ***Agent Policy Set*** view, the created policy set will be immediately applied to the group selected in the directory tree.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Set**.
3. From the directory tree, select the desired group.
4. Click **Create...**.
5. Type the applicable information in the **Policy Set Details** fields.

| Field Name | Type |
|---|---|
| **Policy Set Name** | The name of the agent policy set. |
| **Policy Set Description** | A description of the agent policy set (optional). |

6. Define the **Agent Hardening** option.

   These options define the steps required to delete an agent.

| Option | Description |
|---|---|
| **Agent uninstall protection (list)** | Select from the list to define whether the agent requires a password to be uninstalled. The default value is **On**. |

7. Click **Save**.

**Result:** Your agent policy set is saved and assigned to the selected group. You can also assign the agent policy set to other endpoint groups or edit the set.

## Exporting Agent Policy Set View Data

To export information displayed in the ***Agent Policy Set*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to *Exporting Data* on page 37.

# The Roles View

This view lists the user roles that can access the selected group. This view is similar to the ***Roles*** page, but applies only to the selected group rather than the entire system. From this view, you can manage which group can access the selected group or create new user roles.

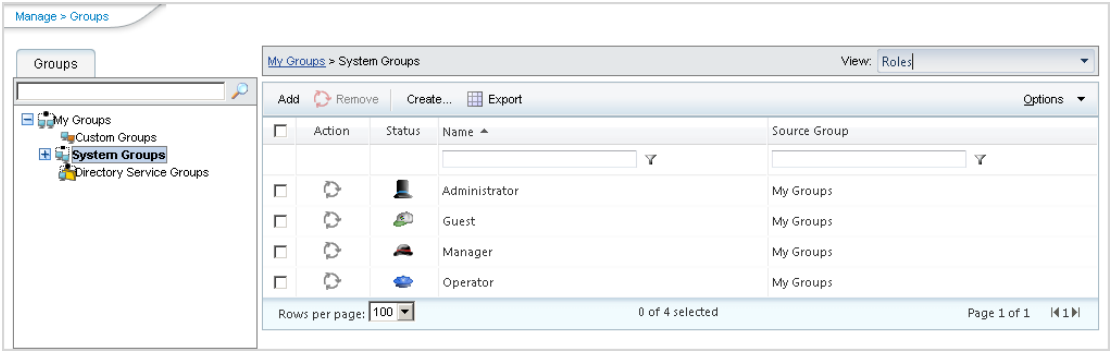



Figure 78: Roles View

## The Roles View Toolbar

This toolbar contains buttons that let you add (or remove) roles that can access the selected group. You can also use it to create new user roles.

The following table describes the functionality of each **Roles** view toolbar button.

Table 85: Roles View Toolbar

| Button | Function |
|---|---|
| **Add** | Adds an established role to the group. For additional information, refer to *Adding a Role to a Group* on page 212. |
| **Remove** | Removes a role from the group. For additional information, refer to *Removing a Role from a Group* on page 213. |
| **Create...** | Creates a new user role. For additional information, refer to *Creating User Roles (Roles View)* on page 214. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |

| Button | Function |
|---|---|
| **Options** (menu) | Opens the **Options** menu. For additional information, refer to *The Options Menu* on page 31. |

## The Roles View List

This list displays the roles that can access the selected group. Use the **Action** column to remove user roles. Additionally, you can filter this table using the filter row.

The following table describes each **Roles** view list column.

Table 86: Roles View List

| Column | Description |
|---|---|
| **Action** | Contains a **Remove** icon. Use this icon to remove a role from the associated role. |
| **Status** | Contains an icon that indicates the type of role. For additional information, refer to one of the following topics:<br>• *Predefined System Roles* on page 262<br>• *Custom Roles* on page 263 |
| **Name** | Indicates the name of the user role. |
| **Source Group** | Indicates the group from which the role was created. |

## Adding a Role to a Group

Add a user role to a group to grant it group access. If the selected group's **Policy inheritance** setting is set to **true**, the added user role will also be able to access the selected group's descendant groups.

Add roles to a group from the ***Roles*** view.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Roles**.
3. Select a group from the directory tree.

4. Click **Add**.

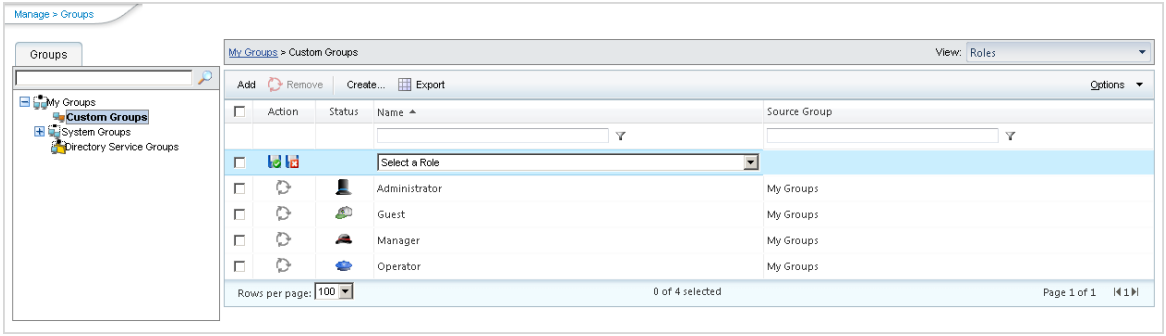



Figure 79: Add a Role

5. Select a role from the **Select a Role** list.
   Select from the following roles:
   - **Administrator**
   - **Manager**
   - **Operator**
   - **Guest**
   - ***Custom Role(s)***

**Note:** ***Custom Role(s)*** are only available if a custom role has been created.

6. Click the **Save** icon.

**Result:** The role is saved and associated with the group.

## Removing a Role from a Group

Remove a user role from a group to deny its associated users group access. If the selected group has **policy inheritance** set to **true**, removing a role will remove the role from the selected group's descendant groups as well.

Remove user roles from a group using the ***Roles*** view.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Roles**.
3. Select a group from the directory tree.
4. Remove roles from the group.
   Use one of the following methods.

| Method | Steps |
|---|---|
| **To remove a single role:** | Click the **Remove** icon associated with the role you want to remove from the group. |

| Method | Steps |
|---|---|
| **To remove multiple roles:** | 1. Select the check boxes associated with the roles you want to remove from the group.<br>2. From the toolbar, click **Remove**. |

**Note:** Inherited roles cannot be removed. To remove inherited roles, either edit the group's inheritence policy or remove the roles from the applicable parent group. To understand group policy inheritance and its effects, refer to *Defining Agent Policy Inheritance Rules* on page 232.

**Step Result:** A dialog displays, asking you to acknowledge the removal.

5. Acknowledge the removal by clicking **OK**.

**Result:** The role is removed and is no longer associated with the group.

## Creating User Roles (Roles View)

Custom roles let you select individual access rights, accessible groups, and accessible endpoints for that role. Create a custom role when predefined system roles do not contain the access rights needed for a particular user. Creating a custom role is also useful when you require a role that can only access specific groups or endpoints.

You can create roles from the ***Roles*** view as well as the ***Roles*** tab.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Roles**.
3. From the directory tree, select the desired group.
4. Click **Create...**.

   **Step Result:** The ***Create Role*** dialog appears with the ***Information*** tab selected by default.

5. Type a name in the **Name** field.
6. Type a description in the **Description** field.
7. Select a role template from the **Role Template** list.

   Any existing role can be used as a template. The selected role determines initial access rights. You can later change which access rights are assigned to the role.
8. Select the ***Access Rights*** tab.
9. Select or clear the desired access rights.

   For additional information, refer to *Predefined System Roles* on page 262.

**Tip:** Select or clear the **All** check box to globally select or clear all access rights. Additionally, child access rights are unavailable until their parent access rights are selected.

10. Select the ***Groups*** tab.

**11.** Assign the desired accessible endpoint groups to the role.

Use one of the following methods to assign groups.

| Method | Steps |
|---|---|
| **To assign individual groups:** | **1.** From the **Available Groups** table, select the check box(es) associated with the group(s) you want to assign.<br>**2.** Click **Assign**. |
| **To assign all groups:** | Click **Assign All**. |

**Tip:** Remove groups using **Remove** and **Remove All**.

**12.** Select the ***Endpoints*** tab.

**13.** Assign the desired accessible endpoints to the role.

Use one of the following methods to assign endpoints.

| Method | Steps |
|---|---|
| **To assign individual endpoints:** | **1.** From the **Available Endpoints** table, select the check box(es) associated with the endpoint(s) you want to assign.<br>**2.** Click **Assign**. |
| **To assign all endpoints:** | Click **Assign All**. |

**Tip:** Remove endpoints using **Remove** and **Remove All**.

**14.** Click **OK**.

**Result:** The new role is saved and assigned to the selected group. It can now be assigned to users. Additionally, it can be edited from the ***Users and Roles*** page ***Roles*** tab.

### Exporting Roles View Data

To export information displayed in the ***Roles*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to *Exporting Data* on page 37.

## The Dashboard View

Similar to the ***Home*** page dashboard, the ***Dashboard*** view displays widgets depicting vulnerability management activity. However, unlike the ***Home*** page dashboard, the ***Dashboard*** view widgets include only information about endpoints within the selected group, its child hierarchy, and their applicable content and packages.

Widgets graphs and information are generated based on the latest Lumension Endpoint Management and Security Suite server and agent data available.

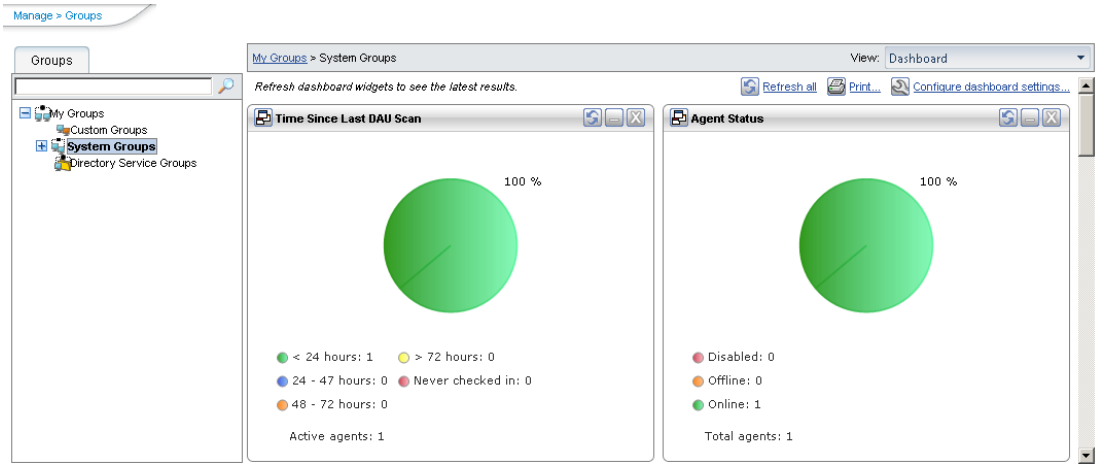



Figure 80: Dashboard View

**Note:** The widgets displayed in the ***Dashboard*** view include data from the selected group's child hierarchy. Configuration changes made to the dashboard settings apply to all groups; not just the selected group.

## Group Dashboard Widgets

The widgets available on the ***Home*** page dashboard are also available from the ***Dashboard*** view. The data depicted on each dashboard changes according to which group is selected.

The following table describes the available widgets.

Table 87: Group Dashboard Widgets

| Widget | Description |
|---|---|
| **Agent Module Installation Status** | Displays the installation and licensing statistic of each agent module. |
| **Agent Status** | Displays all agents grouped by status. |
| **Discovery Scan Results: Agents** | Displays the total number of agent-supported endpoints discovered in the last-run discovery scan job and identifies how many have an agent installed. |

**Tip:** For information about how to edit the group dashboard, refer to *Editing the Dashboard* on page 49.

## Widget Setting and Behavior Icons

Setting and behavior icons are user interface controls that let you manage widgets and the dashboard with the ***Groups*** view. Click these controls to maximize, minimize, hide, and refresh widgets.

The following table describes each icon action.

Table 88: Widget Setting and Behavior Icons

| Icon | Action |
|---|---|
| | Opens the ***Dashboard Settings*** dialog. |
| | Opens the dashboard in print preview mode. |
| | Collapses the associated widget. |
| | Expands the associated collapsed widget. |
| | Hides the associated widget. |
| | Refreshes the associated widget (or the entire dashboard). |

**Note:** Not all widgets contain **Refresh** icons.

## Previewing and Printing the Dashboard

As with the ***Home*** page dashboard, you can preview and print the ***Group*** page ***Dashboard*** view. ***Dashboard*** view widgets display data that applies only to the selected group.

To preview the ***Dashboard*** view, select the applicable group from the **Group Browser Directory** and click the print icon.

For additional information, refer to *Previewing and Printing the Dashboard* on page 49.

## Editing the Dashboard

Just as with the ***Home*** page dashboard, you can edit the widgets displayed on the ***Group*** page ***Dashboard*** view. ***Dashboard*** view widgets display data that only applies to the selected group.

To edit the widgets displayed within the ***Dashboard*** view, select the applicable group from the **Group Browser Directory** and edit icon.

For additional information, refer to *Editing the Dashboard* on page 49.

# The Settings View

This view lets you edit various basic settings for the selected group. These settings impact Mandatory Baselines, agent polices, and so on.

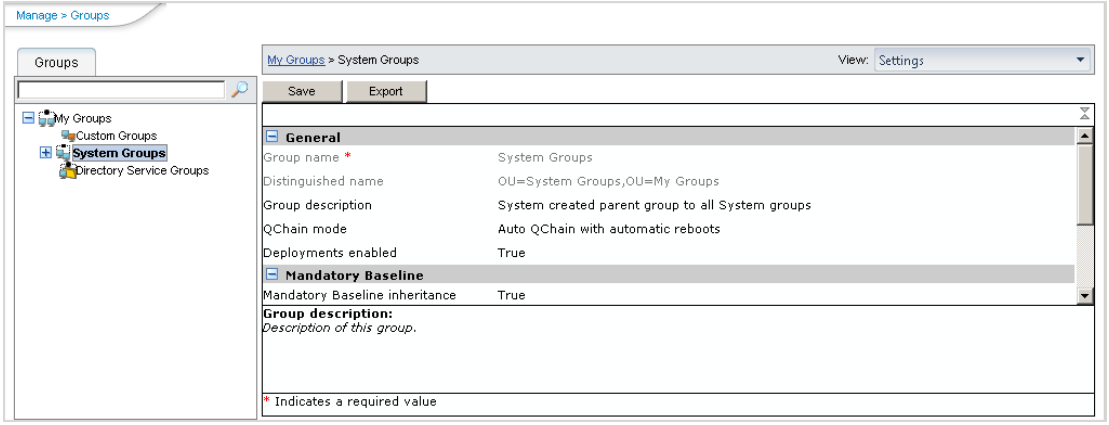



Figure 81: Settings View

The following table describes ***Settings*** view button functions.

Table 89: Settings View Toolbar

| Button | Function |
|---|---|
| **Save** | Saves the settings defined in the page. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |

## Editing Group Settings

If different settings are required, you can edit the default settings for a group. Modifying group settings not only modifies settings for the selected group, but also potentially determines settings for descendant groups.

Modify group settings from the ***Settings*** view.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Settings**.
3. Select the desired group from the directory tree.

4. Under **General**, edit the following options as necessary.

| Option | Description |
|---|---|
| **Group Name (field)** | The group name.<br>**Note:** Only `Custom` group names can be edited. |
| **Distinguished Name** | A system-created group name that represents the group's parent hierarchy.<br>**Note:** The **Distinguished Name** cannot be edited. |
| **Deployments Enabled (list)** **(Patch and Remediation only)** | Defines whether deployments may be created for the group. A `True` value allows authorized users to create deployments for the group. |

5. Under **Policy**, edit the following lists as necessary.

| List | Description |
|---|---|
| **Policy Inheritance** | Defines whether the group inherits the agent policies assigned to the group's parent hierarchy. A `True` value sets the group to inherit its parent hierarchy's agent policy settings.<br>**Note:** To understand agent policy inheritance and its effects, refer to *Defining Agent Policy Inheritance Rules* on page 232. |
| **Policies Enabled** | Defines whether agent policies may be assigned to the group. A `True` value allows users to assign agent policies directly to the group. |

6. Under **Other**, edit the following fields as necessary.

| Field | Description |
|---|---|
| **Group Owners** | User-defined email addresses indicating the owners of the group. |
| **Source Groups (button)** | User-defined group or groups whose agents are dynamically assigned to the group. For additional information, refer to *Assigning a Source Group to a Custom Group* on page 221. |

7. Click **Save**.

**Result:** The new settings are saved and applied to the group.

## Defining Source Groups

*Source groups* are groups that automatically assign managed endpoints to a associated custom group. Use a source group is to maintain multiple endpoint memberships by editing only a single group. This feature simplifies maintenance of endpoint membership among groups.

When working within the ***Groups*** page ***Settings*** view, you can assign the selected view a source group. By assigning the selected group a source group, the selected group will be modified when the source group has endpoints added or removed. Source groups only affect endpoint membership, not group agent policies and settings.

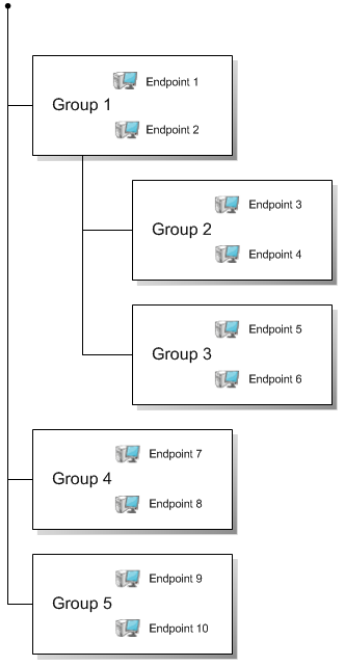



Figure 82: Source Group Diagram

When selecting a source group, all endpoints within the source group's child hierarchy are included, regardless of whether the child groups are selected. Additionally, if the source group (or any of its child groups) has a source group, those endpoints are also included. Source groups can only be assigned to custom groups.

The preceding diagram and the following bullets clarify how group sources operates.

- If group 3 uses group 5 as a source group, then group 3 would include endpoints 9 and 10, as well as endpoints 5 and 6.
- Because group 3 is in group 1's hierarchy, group 1 also includes endpoints 9 and 10.
- If group 4 uses group 1 as a source group, group 4 would include endpoints 7 and 8 (through direct assignment), endpoints 1 and 2 (through a directly assigned source group), endpoints 3, 4, 5, and 6 (through group 1's hierarchy), and endpoints 9 and 10 (through an indirectly assigned source group for [group 5 is a source group for group 3]).

## Assigning a Source Group to a Custom Group

When a custom group is created, you can assign it a *source group*, which is a group that automatically assigns managed endpoints to associated groups. For example, if you assign *Group 1* as a source group to *Group 2*, any agents assigned to *Group 1* are automatically assigned to *Group 2*.

Assign a group a source group from the ***Settings*** view.

**Note:** Source groups can only be assigned to custom groups.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Settings**.
3. Select a custom group from the directory tree.
4. Under **Other**, click **Modify**.

   If necessary, scroll to the button.

   **Step Result:** The ***Edit Source Groups*** dialog opens.

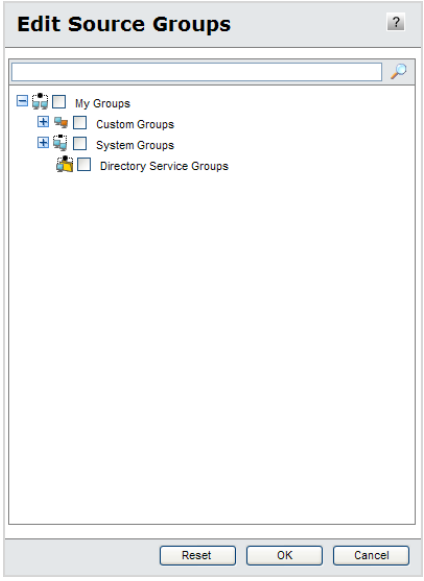



Figure 83: Edit Source Groups Dialog

5. Expand the directory tree or use the search field to locate the group you want to use as a source.
6. Select the check box(es) associated with the group(s) you require as a source.

**Note:** When selecting a source group, all endpoints within the source group's child hierarchy are included, regardless of whether the child groups are selected. Additionally, if the source group (or any of its child groups) has a source group, those endpoints are also included. For additional information, refer to *Defining Source Groups* on page 220.

7. Click **OK**.

**Result:** The custom group now uses the selected group(s) as its source. As new agents are added to (or removed from) the source group, they are also added to (or removed from) the custom group.

## Exporting Settings View Data

To export information displayed in the ***Settings*** view to a comma separated value (`.csv`) file, click **Export**. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to *Exporting Data* on page 37.

# Chapter 9

# Managing Agent Policy Sets

**In this chapter:**


- The Agent Policy Sets Page
- Working with Agent Policy Sets


Use *agent policy sets* to control agent behavior. These sets are composed of policies, which define how individual agent functions behave.

Apply agent policy sets to groups to implement your policies. There is a policy for every agent function.

## The Agent Policy Sets Page

You can govern how agents behave by creating and assigning agent policy sets. Use the ***Agent Policy Sets*** page to define agent rules of behavior.

You can access this page at any time from the navigation menu.

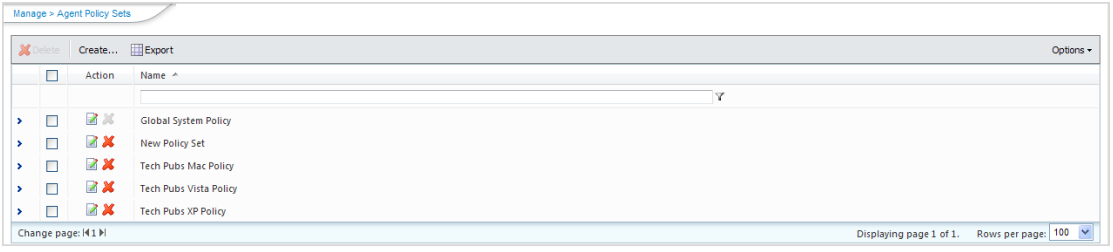



Figure 84: Agent Policy Sets Page

### About Agent Policies and Agent Policy Sets

*Agent policies* govern agent operations. With agent policies, you can control all aspects of agent behavior. Assign agent policies to endpoint groups via *agent policy sets*, which are a collection of agent policy values.

Based on group membership, agents operate according to assigned agent policy values. Assignment of agent policy sets is optional. Groups without assigned policy sets or policies have their behavior defined by the **Global System Policy**. This policy set:

- Defines behavior for groups with no assigned policy set.
- Defines policy values for incomplete agent policy sets.

When agents holding multiple group memberships are assigned conflicting agent policy values, they are resolved with conflict resolution rules. These rules are a set of protocols that determine which policy value an agent uses

when conflicts occur. For additional information, refer to *Defining Agent Policy Conflict Resolution* on page 232.

## Viewing the Agent Policy Sets Page

Navigate to this page to view agent policy sets.

You can access this page any time using the navigation menu.

1. Select **Manage** > **Agent Policy Sets**.

   **Step Result:** The ***Agent Policy Sets*** page opens.

2. If desired, complete a task listed in *Working with Agent Policy Sets* on page 226.

## The Agent Policy Sets Page Toolbar

This toolbar contains buttons that lets you create and edit agent policy sets.

The following table describes each toolbar button.

Table 90: Agent Policy Sets Page Toolbar

| Button | Function |
|---|---|
| **Delete** | Deletes the selected agent policy set(s). For additional information, refer to *Deleting an Agent Policy Set* on page 228. |
| **Create...** | Creates a new agent policy set. For additional information, refer to *Creating an Agent Policy Set* on page 226. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |
| **Options** (menu) | Opens the **Options** menu. For additional information, refer to *The Options Menu* on page 31. |

## The Agent Policy Sets Page List

For each agent policy set that you create, an item for that set appears in the ***Agent Policy Sets*** page list. This list names each existing agent policy set and provides access to editing functionality.

The following table describes each list column.

Table 91: Agent Policy Sets Page List

| Column | Description |
|---|---|
| **Action** | Contains **Edit** and **Delete** icons. Use these icons to edit and delete the associated agent policy set. For additional information, refer to the following topics:<br>• *Editing an Agent Policy Set* on page 227<br>• *Deleting an Agent Policy Set* on page 228<br>**Note:** The **Global System Policy** cannot be deleted. |
| **Name** | The name of the agent policy set. |

Each item listed on the ***Agent Policy Sets*** page can be expanded, providing details about the applicable agent policy settings. Viewing agent policy set details from this list is faster than viewing them in the ***Edit Agent Policy Set*** dialog. To view agent policy set details from the page list, click the **Rotating Chevron** (>) associated with the applicable agent policy set, which opens a table containing additional details.

The following reference describes each column in the agent policy sets details table.

Table 92: Agent Policy Set Details Table

| Name | Description |
|---|---|
| **Policy Name** | Indicates the unique name of the agent policy set. |
| **Type** | Indicates the type of agent policy set (`System` or `User Defined`). |
| **Description** | Indicates the description of the agent policy set. |
| **Created By** | Indicates the name of the user that created the agent policy set. |
| **Created Date** | Indicates the date and time that the agent policy set was created. |
| **Modified By** | Indicates the name of the user that last modified the agent policy set. |
| **Modified Date** | Indicates the date and time that the agent policy set was last modified. |

**Note:** This reference table does not list the **Value** contained in the agent policy set details. This column (which appears in the user interface) contains values that agent policies are set to.

# Working with Agent Policy Sets

There are many tasks that you can perform from the ***Agent Policy Sets*** page related to agent policy sets. Some tasks are performed by clicking toolbar buttons, while others are performed by interacting with list items.


- *Creating an Agent Policy Set* on page 226
- *Editing an Agent Policy Set* on page 227
- *Deleting an Agent Policy Set* on page 228
- *Defining the Global Uninstall Password* on page 229
- *Defining Agent Policy Logging Levels* on page 230
- *Defining Agent Policy Conflict Resolution* on page 232
- *Exporting Agent Policy Set Data* on page 233


## Creating an Agent Policy Set

Within Lumension Endpoint Management and Security Suite (Lumension EMSS), you can create a limitless number of agent policy sets to define how agents behave. Following creation, associate a policy set with a group or endpoint to apply policy settings. After installing Patch and Remediation, new Patch and Remediation options are available when creating an agent policy set.

Create agent policy sets from the ***Create Agent Policy Set*** dialog.

1. Select **Manage** > **Agent Policy Sets**.
2. Click **Create...**.

   **Step Result:** The ***Create Agent Policy Set*** dialog opens.

3. Type the applicable information in the **Policy Set Details** fields.

| Field Name | Type |
|---|---|
| **Policy Set Name** | The name of the agent policy set. |
| **Policy Set Description** | A description of the agent policy set (optional). |

4. Define the **Agent Hardening** option.

   These options define the steps required to delete an agent.

| Option | Description |
|---|---|
| **Agent uninstall protection (list)** | Select from the list to define whether the agent requires a password to be uninstalled. The default value is **On**. |

5. Define the **Agent Logging** options.

   The following table describes each option.

| Option | Step |
|---|---|
| **Logging level (button)** | Click to open the ***Logging Level*** dialog. Use this dialog to select the agent logging level. For additional information, refer to *Defining Agent Policy Logging Levels* on page 230. |
| **Maximum log file size (field)** | Type the amount of diskspace that triggers the agent to delete its log (1-500 MB). A value of *10* is the default setting. |

6. Click **Save**.

**Result:** Your agent policy set is saved. You can now assign the agent policy set to endpoint groups or edit the set.

**After Completing This Task:**

To assign an agent policy set to a group, complete *Assigning an Agent Policy Set to a Group* on page 209.

## Editing an Agent Policy Set

Following the creation of an agent policy set, you can modify a policy set to suit your needs as endpoints and groups change within Lumension Endpoint Management and Security Suite (Lumension EMSS).

The ***Edit A Policy Set*** dialog allows you to modify an agent policy set.

1. Select **Manage** > **Agent Policy Sets**.
2. Click the **Edit** icon associated with the policy set you want to edit.

   **Step Result:** The ***Edit a Policy Set*** dialog opens.

3. If desired, edit the **Policy Set Details** fields.

| Field Name | Type |
|---|---|
| **Policy Set Name** | The name of the agent policy set. |
| **Policy Set Description** | A description of the agent policy set (optional). |

4. If desired, edit the **Agent Hardening** options.

| Option | Step |
|---|---|
| **Agent uninstall protection (list)** | Select from the list to define whether the agent requires a password to be uninstalled. The default value is **On**. |

| Option | Step |
|---|---|
| **Global Uninstall Password (button)** | Click **Modify** to open the ***Global Uninstall Password*** dialog. Use this dialog to define a password for manually uninstalling the agent. For additional information, refer to *Defining the Global Uninstall Password* on page 229.<br>**Note:** This option is only available when editing the Global System Policy agent policy set. |

5. If desired, edit the **Agent Logging** options.

| Option | Step |
|---|---|
| **Logging level (button)** | Click to open the ***Logging Level*** dialog. Use this dialog to select the agent logging level. For additional information, refer to *Defining Agent Policy Logging Levels* on page 230. |
| **Maximum log file size (field)** | Type the amount of diskspace that triggers the agent to delete its log (1-500 MB). A value of *10* is the default setting. |

6. If desired, edit the **Agent Communication** option.
7. Click **Save**.

**Result:** Your edits are saved. The new policy values take effect the next time the applicable agents communicate with the Lumension EMSS server.

## Deleting an Agent Policy Set

As your network environment changes, agent policy sets may no longer be applicable. When this event occurs, delete the unnecessary policy set.

You can delete agent policy sets at any time from the ***Agent Policy Sets*** page.

1. Select **Manage** > **Agent Policy Sets**.
2. Delete one or more agent policy set.

   Use one of the following methods.

| Method | Steps |
|---|---|
| **To delete one agent policy set:** | Click the **Delete** icon associated with an agent policy set. |

| Method | Steps |
|---|---|
| **To delete multiple agent policy sets:** | 1. Select the check boxes associated with the agent policy sets you want to delete.<br>2. From the toolbar, click the **Delete** button. |

**Note:** Assigned agent policy sets and the **Global System Policy** cannot be deleted.

**Step Result:** A dialog displays, asking you to acknowledge the deletion.

3. Acknowledge the deletion by clicking **OK**.

**Result:** The agent policy set is deleted.

## Defining the Global Uninstall Password

To uninstall a Lumension Endpoint Management and Security Suite (Lumension EMSS) Agent from its host endpoint, you must enter one of two passwords: the password specific to that endpoint, or the global uninstall password. You can use the global uninstall password to uninstall any Lumension EMSS agent registered to your Lumension EMSS server. This feature ensures that endpoint users cannot uninstall the agent without the knowledge and permission of a network administrator.

Define the global uninstall password when editing the **Global System Policy**.

1. Select **Manage** > **Agent Policy Sets**.
2. Click the edit icon associated with the global system policy set.

   **Step Result:** The ***Edit a Policy Set*** dialog opens.

3. Under the ***Agent Hardening*** section, click the **Modify** button adjacent to the **Global uninstall password** field.

   **Step Result:** The ***Global Uninstall Password*** dialog opens.

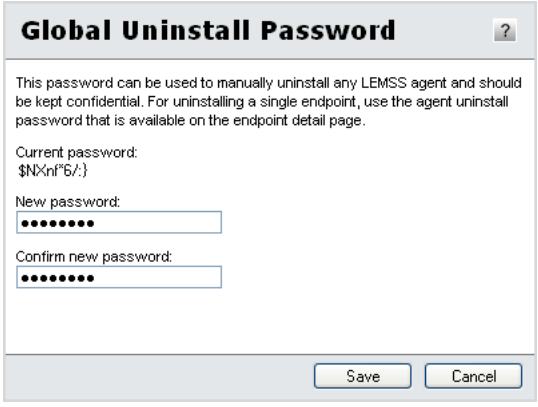

Global Uninstall Password
This password can be used to manually uninstall any LEMSS agent and should be kept confidential. For uninstalling a single endpoint, use the agent uninstall password that is available on the endpoint detail page.
Current password:
$NXnf"6/:}
New password:
Confirm new password:
Save
Cancel

Figure 85: Global Uninstall Password Dialog

4. Type the desired password in the **New password** field.
5. Retype the password in the **Confirm new password** field.

6. Click **Save**.
7. Finish any desired edits to the agent policy set and click **Save**.

**Result:** The ***Global Uninstall Password*** dialog closes. Your edits take effect the next time Lumension EMSS and the applicable agents communicate.

**Note:** Password edits are not saved until the agent policy set itself is saved.

## Defining Agent Policy Logging Levels

All Lumension Endpoint Management and Security Suite Agents record a log of events that transpire on their host endpoint. An agent policy set's logging level setting controls how much memory an agent's host endpoint allocates for event logs. Define logging levels carefully: a low logging level may not record enough information to be useful; however, a high logging level may record verbose information at the cost of higher disk space.

Define logging levels when creating or editing an agent policy set.

1. Select **Manage** > **Agent Policy Sets**.
2. Perform one of the following procedures based on your context.

| Context | Procedure |
|---|---|
| **If you are creating an agent policy set:** | Click **Create...**. |
| **If you are editing an agent policy set:** | Click the edit icon associated with the policy set containing the logging level setting you want to edit. |

**Step Result:** Either the ***Create Agent Policy Set*** or the ***Edit a Policy Set*** dialog opens.

3. Under the ***Agent Logging*** section perform one of the following procedures based on your context.

| Context | Procedure |
|---|---|
| **If you are defining the logging level for the first time:** | Click the **Define** button adjacent to the **Logging level** field. |

| Context | Procedure |
|---|---|
| **If you are modifying the logging level:** | Click the **Modify** button adjacent to the **Logging level** field. |

**Step Result:** The ***Logging Level*** dialog opens.

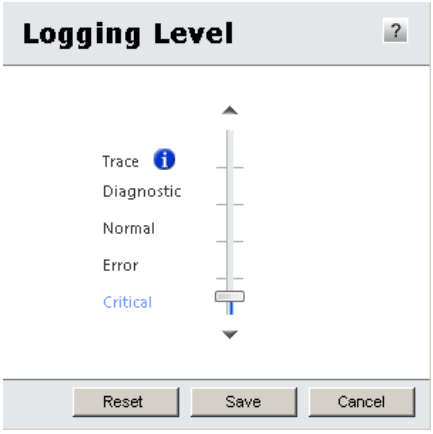



Figure 86: Logging Level Dialog

4. Move the slider to the desired logging level.
   The following table describes each logging level.

| Logging Level | Description |
|---|---|
| **Trace** | Logs all errors and system actions. |
| **Diagnostic** | Logs all errors and major system actions. |
| **Normal** | Logs all errors and basic system action and usage information. |
| **Error** | Logs only errors. |
| **Critical** | Logs only critical events. |

5. Click **Save**.
6. Finish any additional edits to the agent policy set and click **Save**.

**Result:** The ***Logging Level*** dialog closes. Your edits take effect the next time the Lumension Endpoint Management and Security Suite server and the applicable agents communicate.

**Note:** Logging level edits are not saved until the agent policy set itself is saved.

## Defining Agent Policy Inheritance Rules

A group's behavior is defined via an agent policy set, which can be assigned directly to the group or inherited using a group's **Policy inheritance** setting.

Because a group can inherit policies and have them directly assigned, policy conflicts may arise. The following rules apply when a group has **Policy Inheritance** set to `True`:

1. Any conflicting policies that are assigned to the parent, but not the child, are resolved at the parent level per the conflict policy resolution rules.
2. Agent policy set values assigned directly to a group supersede inherited agent policy set values.
3. Any conflicting policies that are assigned directly to the child group are resolved per the conflict resolution rules.
4. Any agent policy set values that are undefined by the group's directly assigned policy are defined by the parent's group policy.
5. Policy values still undefined are defined by the global system policy set.

For more information on how to enable a group's **Policy inheritance** setting, refer to *Editing Group Settings* on page 218.

For more information on conflict policy resolution rules, refer to *Defining Agent Policy Conflict Resolution* on page 232.

## Defining Agent Policy Conflict Resolution

On occasion, a group or endpoint may be assigned two different agent policy sets that have conflicting settings. When this occurs, the system determines which of the conflicting settings to use based on *agent policy conflict resolution*, which is a series of protocols that determine which settings take priority.

Conflicting policies are resolved in the following order.

1. **Group Policies** - Conflicting policy sets assigned to a group are resolved before conflicting policy sets assigned to an agent are resolved.

   The following rules apply if a group has **Policy Inheritance** set to `False`:

   a. The applicable group does not inherit its parent's policy set. Therefore, only policy sets assigned directly to the group require resolution.
   b. Conflicting policy set values are resolved according to the agent policy conflict resolution rules.

   The following rules apply if a group has **Policy Inheritance** set to `True`:

   a. The applicable child group inherits its parent's policy set. Any conflicting policy sets that are assigned to the parent, not the child, are resolved at the parent level.
   b. Conflicting policy sets assigned directly to the child group are resolved according to the agent policy conflict resolution rules. Policy set values assigned directly to a group supersede inherited policy set values.
   c. Finally, any policy set values that are undefined by the group's directly assigned policy are defined by the parent's group policy (if defined by the parent group).
2. **Agent Policies** - After resolving the group policies, the conflicting policies assigned to an agent (via its group membership) are resolved. The following rules apply:

a. The resultant policies of all groups to which the agent is a member are resolved according to the agent policy conflict resolution rules.
b. Any policy values that have not been defined via the agent's group membership are populated based on the policy settings defined in the **Global Policy Set**.

**Note:** The **Global Policy Set** policy values are used to fill undefined values in other agent policy sets. Therefore, conflict resolution rules do not apply to the **Global Policy Set**.

The following table defines the rules used when resolving conflicting policy settings:

Table 93: Agent Policy Conflict Resolution Rules

| Policy Setting | Resolution |
|---|---|
| **Agent Hardening** | The agent uses the `On`. |
| **Agent Version** | The newest version of the agent must be installed. |
| **Logging Level** | The agent uses the most comprehensive **Logging Level** (Debug > Detailed > Basic Information). |
| **Agent Scan Mode** | The agent uses the fastest **Agent Scan Mode** (Fast Scan > Initial Scan > Normal Scan). |
| **Communication Interval** | The agent uses the shortest **Communication Interval**. |
| **Agent Listener Port** | If any group has an agent listener port defined (not *0* ), the agent listens on the highest defined port. |

## Exporting Agent Policy Set Data

To export the list of agents policy sets listed on the ***Agent Policy Sets*** page to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with data in other programs for reporting and analytical purposes.

Data for policy values are also exported. For additional information, refer to *Exporting Data* on page 37.

## Assigning an Agent Policy Set to a Group

Associating an agent policy set with a group defines functional rules for the group to follow. Groups that do not have an associated agent policy set use the **Global System Policy**.

**Prerequisites:**

Create an agent policy set.

Assign agent policy sets to a group from the ***Agent Policy Set*** view.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Set**.
3. Select a group from the directory tree.
4. Click **Assign**.

5. Select an agent policy set from the **Select a Policy Set** list.
6. Click the **Save** icon.

**Result:** The policy set is saved and associated with the group.

## Removing an Agent Policy Set from a Group

When desired, you can remove an agent policy set from a group. Groups without associated policy sets use the global system policy to define their behavior.

Remove agent policy sets from a group from the ***Agent Policy Sets*** view.

**Note:** You cannot remove inherited policy sets. Instead, you must change the group's policy inheritance setting or remove the inherited policy set from the parent group.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Sets**.
3. Select a group from the directory tree.
4. Remove the desired policy sets.

   Use one of the following methods.

| Method | Steps |
|---|---|
| **To remove one agent policy set:** | Click the **Remove** icon associated with the policy set you want to remove. |
| **To remove multiple agent policy sets:** | 1. Select the check boxes associated with the agent policy sets you want to remove.<br>2. From the toolbar, click **Remove**. |

   **Step Result:** A dialog appears, asking you to acknowledge the removal.

5. Acknowledge the removal by clicking **OK**.

**Result:** The agent policy set is no longer associated with the group and is removed from the ***Agent Policy Set*** view.

# Chapter 10

# Reporting

**In this chapter:**


- About Reports
- The All Reports Page
- Generating a Report
- Working with HTML Reports
- Working with PDF Reports
- Available Reports


Lumension Endpoint Management and Security Suite can generate a variety of reports summarizing network conditions.

Use these reports for internal reporting, management briefing, and assistance when using Lumension Endpoint Management and Security Suite.

## About Reports

*Reports* are records that document activity and information pertaining to your network environment.

Lumension Endpoint Management and Security Suite offers multiple predefined report templates that list and/or depict data collected during network management. Data included in these reports range from general (endpoints, discovery scan jobs) to highly detailed (operating systems installed on network endpoint). Reports are created by selecting a report type and defining its parameters.

Additionally, report formats vary. Some reports are in a HTML (`.html`) file format, while others are in a PDF (`.pdf`) format.

# The All Reports Page

From this page, you can generate all available reports. Use this page to generate reports related Lumension Endpoint Management and Security Suite's various functions. Before generating the report, select the report type and define the report parameters.

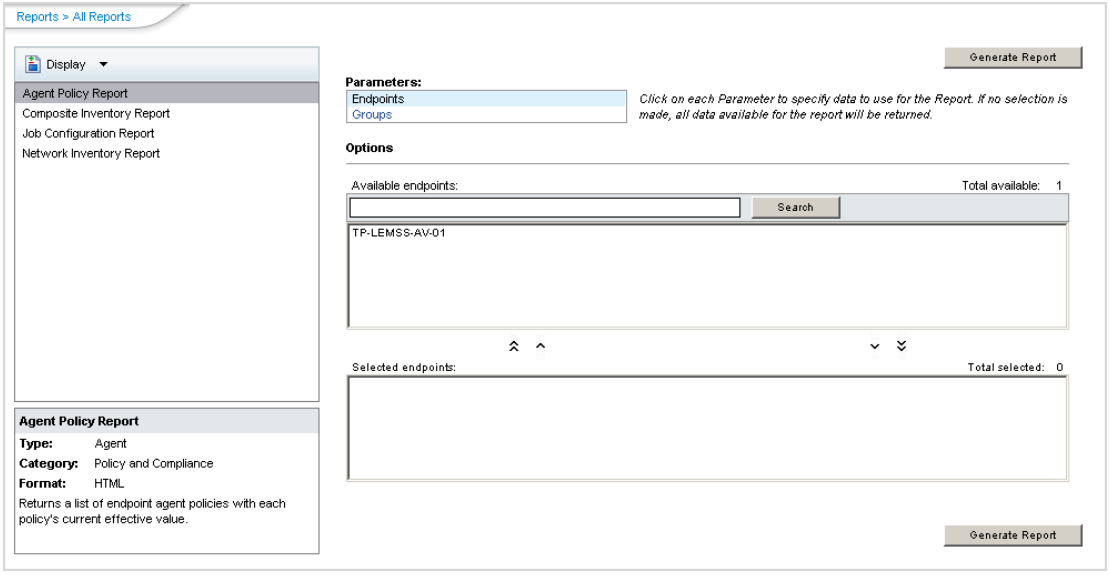



Figure 87: All Reports Page

**Note:** From the **Reports** menu, you can select multiple ***All Reports*** page variants. Based on which **Reports** menu item you select, the resulting page that opens groups its **Display** menu differently. For example, selecting **Reports** > **Configuration** opens a reports page containing a **Display** menu with an expanded **Configuration** group. See the following table for a description of each **Reports** menu command.

Table 94: Reports Menu Commands

| Command | Description |
|---|---|
| **All Reports** | Displays all reports ungrouped. |
| **Configuration** | Reports are grouped with the **Configuration** group expanded. Configuration reports display information about agent and job configurations. |
| **Management/Status** | Reports are grouped with the **Management/Status** group expanded. These reports display information related to content deployments. |

## Viewing the All Reports Page

Navigate to this page to generate either HTML or PDF reports.

Access this page from the navigation menu.

1. Select **Reports** > **All Reports**.
2. Generate the desired report.

## The Display List

This list displays all reports for generation. To generate a report, select it from the list.

If you select an ***All Reports*** page variant, the **Display** list items are grouped in a directory tree structure.

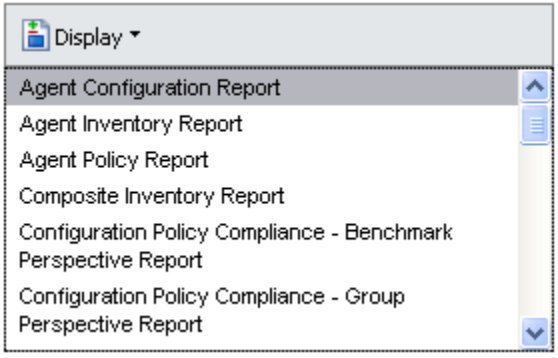



Figure 88: Display List

Additionally, the **Display** list contains the **Display** menu, which appears in the list's header. This menu lets you reorganize list items alphabetically or in a grouped directory tree structure. The following table describes each **Display** menu item.

Table 95: Display Menu Items

| Item | Description |
|---|---|
| **Sort Ascending** | Sorts **Display** list items and/or groups in ascending alphabetical order. This item is selected by default. |
| **Sort Descending** | Sorts **Display** list items and/or groups in descending alphabetical order. |
| **All** | Lists all available reports in an ungrouped format. |
| **Categories** | Groups reports into different expandable and collapsible categories. This item is selected by default. |

### The Report Description

The report description summarizes the report selected from the **Display** list. Read this for a brief overview of the report you have selected.

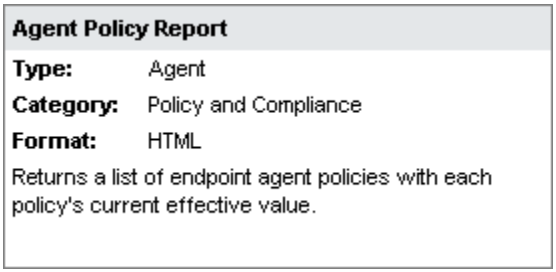

Agent Policy Report
Type: Agent
Category: Policy and Compliance
Format: HTML
Returns a list of endpoint agent policies with each policy's current effective value.

Figure 89: Report Description

The following table describes the fields that appear in the report description, including the header.

Table 96: Report Description Fields

| Field | Description |
|---|---|
| ***Report Description Header*** | The name of the report currently selected from the **Display** list. |
| **Type** | The data source of the report. Report data derives from either agents or network-based scans (discovery scan jobs). |
| **Category** | The category of the report. |
| **Format** | The format of the report (`PDF` or `HTML`). |

## Generating a Report

Lumension Endpoint Management and Security Suite provides multiple predefined reports. These reports comprehensively detail your computing environment, reflecting your content and vulnerability management activities. Generate reports to brief management or to view network behavior and statistics.

Generate reports from the ***All Reports*** page.

1. Select **Reports** > **All Reports**.
2. From the **Display** list, select the report you want to generate.
3. Using one of the following methods, select the required report parameters.
   - Add parameters to the **Selected Parameters** list using the **Include** or **Include All** arrows.
   - Select parameters from the available drop-down lists, data grids, or list boxes.

**Note:** Refer to *Available Core Reports* on page 240 and the individual report descriptions for details regarding which parameters are required and which parameters are optional.

4. If desired, select the optional report parameters.
5. Click **Generate Report**.

**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses pop-up windows from appearing and must be disabled to display report data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress report display functionality and should be disabled.

**Result:** The report is generated in a new window.

# Working with HTML Reports

After generating an HTML report, the report opens in a new window. Within this window, you can perform a number of tasks specific to the report.


- *Displaying Time and Date in HTML Reports* on page 239
- *Exporting HTML Reports* on page 239
- *Previewing and Printing HTML Reports* on page 240


## Displaying Time and Date in HTML Reports

Some HTML reports generate date range data. For these reports, you can change how this data is formatted: either by local time or Coordinated Universal Time.

The following table describes the options for displaying date and time information.

Table 97: HTML Report Time and Date Display Options

| Option | Description |
|---|---|
| **Local Time** | The date and time established by the Lumension Endpoint Management and Security Suite Server. |
| **UTC Time** | Coordinated Universal Time. Also known as Universal Time, Zulu Time, or Greenwich Mean Time. |

## Exporting HTML Reports

After generating an HTML, you can export its data values into other file formats. You can then edit this data using other applications.

Once the HTML (`.html`) report is created, you have the option of exporting the report into another file format.

Reports are presented in standard HTML (`.html`) and can be exported into several file formats for your convenience.

- Comma Separated Values (`.CSV`)
- Microsoft Excel Worksheet (`.XLS`)
- XML Document

To export the report, select an option from the list and click **Export**.

**Note:** All data results will export, not just selected results. However, some of the data may not export in a readable format.

### Previewing and Printing HTML Reports

After generating a HTML (`.html`) report, you can format it specifically for printing. Use this feature before printing a report rather than using your Web browser print feature.

**Prerequisites:**

Generate a report.

1. Click the **Printer-friendly Version** link.

   **Step Result:** The report refreshes with the data in print preview mode.

2. If desired, click the **Send to Printer** link to print the report.

**Result:** The ***Print*** dialog opens. Finish printing your report by completing the ***Print*** dialog.

**Note:** If printer connectivity is not established, you cannot print your report. Complete the ***Add Printer Wizard*** prior to printing reports if needed.

## Working with PDF Reports

After generating a PDF (`.pdf`) report, you can view it within a PDF reader.

To generate a PDF (`.pdf`) report, you must have Adobe® Reader® (or another PDF reader such as Foxit® Reader®) installed on your computer. When reading a generated report, the functions of these programs aid your report viewing.

For more information on using Adobe Reader, see the *Adobe Reader 8 User Guide*.

## Available Reports

Lumension Endpoint Management and Security Suite features a variety of reports. Each report documents Lumension Endpoint Management and Security Suite activities and statistics.

The reports available for generation change based on which modules you have installed.


- *Available Core Reports* on page 240


### Available Core Reports

Lumension Endpoint Management and Security Suite (Lumension EMSS) provides various HTML- and PDF-formatted reports, which list comprehensive information about Lumension EMSS.

The following reports are available within Lumension EMSS when no modules are installed.


- *Agent Policy Report* on page 241
- *Composite Inventory Report* on page 241
- *Job Configuration Report* on page 243
- *Network Inventory Report* on page 246

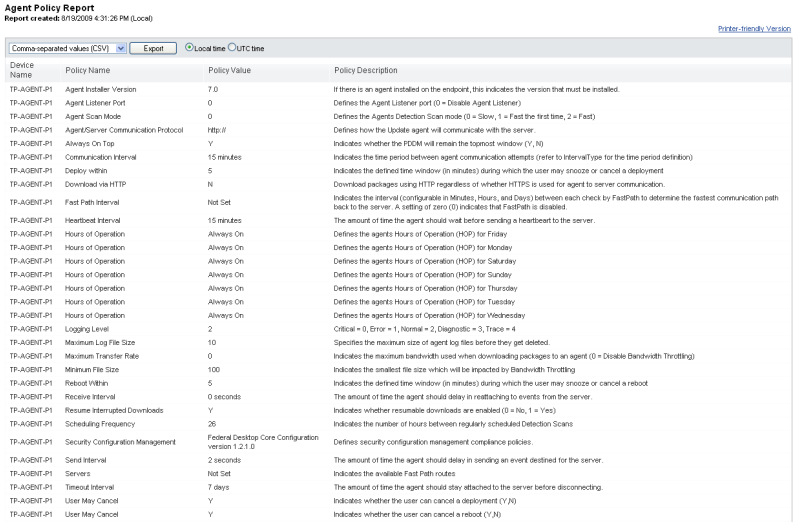
## Agent Policy Report

This report shows the policies that are the resolution of all policies assigned to the endpoint. In the report, each policy value is listed in the **Policy Name** column. When using groups as a parameter to select multiple endpoints, the group policies are not part of the actual results.

**Optional Parameters**: `Endpoints`, `Groups`

**Note:** If no parameter selection is made, the report generates using all available data.

The following table describes each report field.



**Agent Policy Report**
**Report created:** 8/19/2009 4:31:26 PM (Local)

Printer-friendly Version

Comma-separated values (CSV) | Export | Local time | UTC time

| Device Name | Policy Name | Policy Value | Policy Description |
|---|---|---|---|
| TP-AGENT-P1 | Agent Installer Version | 7.0 | If there is an agent installed on the endpoint, this indicates the version that must be installed. |
| TP-AGENT-P1 | Agent Listener Port | 0 | Defines the Agent Listener port (0 = Disable Agent Listener) |
| TP-AGENT-P1 | Agent Scan Mode | 0 | Defines the Agents Detection Scan mode (0 = Slow, 1 = Fast the first time, 2 = Fast) |
| TP-AGENT-P1 | Agent/Server Communication Protocol | http:// | Defines how the Update agent will communicate with the server. |
| TP-AGENT-P1 | Always On Top | Y | Indicates whether the PDDM will remain the topmost window (Y, N) |
| TP-AGENT-P1 | Communication Interval | 15 minutes | Indicates the time period between agent communication attempts (refer to IntervalType for the time period definition) |
| TP-AGENT-P1 | Deploy within | 5 | Indicates the defined time window (in minutes) during which the user may snooze or cancel a deployment |
| TP-AGENT-P1 | Download via HTTP | N | Download packages using HTTP regardless of whether HTTPS is used for agent to server communication. |
| TP-AGENT-P1 | Fast Path Interval | Not Set | Indicates the interval (configurable in Minutes, Hours, and Days) between each check by FastPath to determine the fastest communication path back to the server. A setting of zero (0) indicates that FastPath is disabled. |
| TP-AGENT-P1 | Heartbeat Interval | 15 minutes | The amount of time the agent should wait before sending a heartbeart to the server. |
| TP-AGENT-P1 | Hours of Operation | Always On | Defines the agents Hours of Operation (HOP) for Friday |
| TP-AGENT-P1 | Hours of Operation | Always On | Defines the agents Hours of Operation (HOP) for Monday |
| TP-AGENT-P1 | Hours of Operation | Always On | Defines the agents Hours of Operation (HOP) for Saturday |
| TP-AGENT-P1 | Hours of Operation | Always On | Defines the agents Hours of Operation (HOP) for Sunday |
| TP-AGENT-P1 | Hours of Operation | Always On | Defines the agents Hours of Operation (HOP) for Thursday |
| TP-AGENT-P1 | Hours of Operation | Always On | Defines the agents Hours of Operation (HOP) for Tuesday |
| TP-AGENT-P1 | Hours of Operation | Always On | Defines the agents Hours of Operation (HOP) for Wednesday |
| TP-AGENT-P1 | Logging Level | 2 | Critical = 0, Error = 1, Normal = 2, Diagnostic = 3, Trace = 4 |
| TP-AGENT-P1 | Maximum Log File Size | 10 | Specifies the maximum size of agent log files before they get deleted. |
| TP-AGENT-P1 | Maximum Transfer Rate | 0 | Indicates the maximum bandwidth used when downloading packages to an agent (0 = Disable Bandwidth Throttling) |
| TP-AGENT-P1 | Minimum File Size | 100 | Indicates the smallest file size which will be impacted by Bandwidth Throttling |
| TP-AGENT-P1 | Reboot Within | 5 | Indicates the defined time window (in minutes) during which the user may snooze or cancel a reboot |
| TP-AGENT-P1 | Receive Interval | 0 seconds | The amount of time the agent should delay in reattaching to events from the server. |
| TP-AGENT-P1 | Resume Interrupted Downloads | Y | Indicates whether resumable downloads are enabled (0 = No, 1 = Yes) |
| TP-AGENT-P1 | Scheduling Frequency | 26 | Indicates the number of hours between regularly scheduled Detection Scans |
| TP-AGENT-P1 | Security Configuration Management | Federal Desktop Core Configuration version 1.2.1.0 | Defines security configuration management compliance policies. |
| TP-AGENT-P1 | Send Interval | 2 seconds | The amount of time the agent should delay in sending an event destined for the server. |
| TP-AGENT-P1 | Servers | Not Set | Indicates the available Fast Path routes |
| TP-AGENT-P1 | Timeout Interval | 7 days | The amount of time the agent should stay attached to the server before disconnecting. |
| TP-AGENT-P1 | User May Cancel | Y | Indicates whether the user can cancel a deployment (Y,N) |
| TP-AGENT-P1 | User May Cancel | Y | Indicates whether the user can cancel a reboot (Y,N) |

Figure 90: Agent Policy Report

Table 98: Agent Policy Report Column Definitions

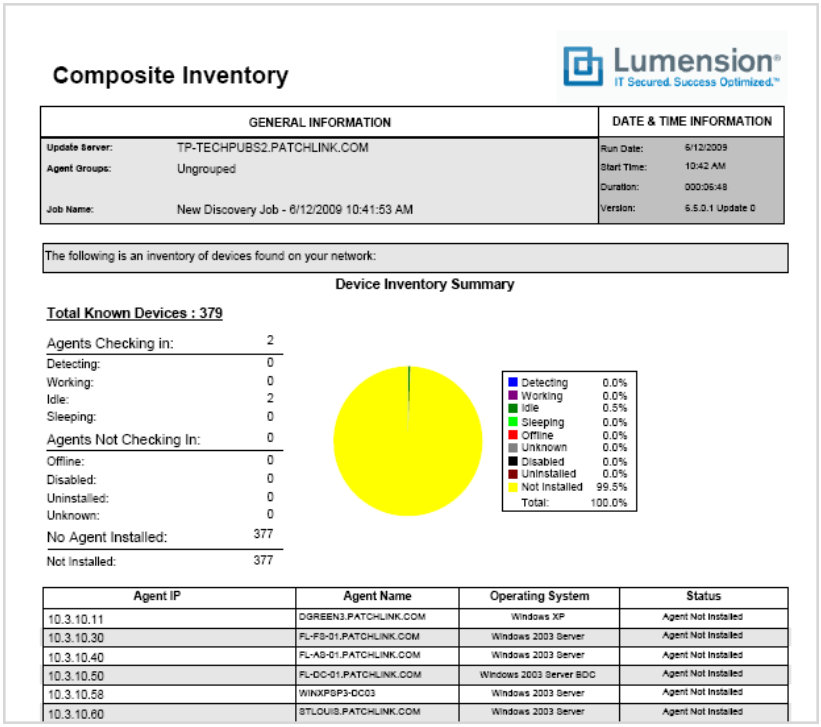
| Column | Definition |
|---|---|
| **Endpoint Name** | The name of the endpoint. |
| **Policy Name** | The name of the agent policy. |
| **Current Value** | The policy setting. |
| **Policy Desc** | The agent policy's description. |

## Composite Inventory Report

This report lists details for endpoints associated with the specified agent groups and job (discovery scan or agent management). This report includes a pie chart that shows the agent status counts for the agent groups and scan job. A `Not Installed` agent status assigned to an endpoint that exists only in the job and not a selected agent group. Details are also displayed for each endpoint.

**Required Parameters**: Selection of one or multiple `agent group(s)` and one `completed job`.

**Optional Parameters** (default setting): `Sort by` (IP address, machine name, operating system [OS]), `Included OSs`, `Included IP addresses`.



Composite Inventory

Lumension® IT Secured. Success Optimized.™

| GENERAL INFORMATION | | DATE & TIME INFORMATION | |
|---|---|---|---|
| Update Server: | TP-TECHPUBS2.PATCHLINK.COM | Run Date: | 6/12/2009 |
| Agent Groups: | Ungrouped | Start Time: | 10:42 AM |
| | | Duration: | 000:06:48 |
| Job Name: | New Discovery Job - 6/12/2009 10:41:53 AM | Version: | 6.5.0.1 Update 0 |

The following is an inventory of devices found on your network:

Device Inventory Summary

Total Known Devices : 379

| | |
|---|---|
| Agents Checking in: | 2 |
| Detecting: | 0 |
| Working: | 0 |
| Idle: | 2 |
| Sleeping: | 0 |
| Agents Not Checking In: | 0 |
| Offline: | 0 |
| Disabled: | 0 |
| Uninstalled: | 0 |
| Unknown: | 0 |
| No Agent Installed: | 377 |
| Not Installed: | 377 |



| Agent IP | Agent Name | Operating System | Status |
|---|---|---|---|
| 10.3.10.11 | DGREEN3.PATCHLINK.COM | Windows XP | Agent Not Installed |
| 10.3.10.30 | FL-FS-01.PATCHLINK.COM | Windows 2003 Server | Agent Not Installed |
| 10.3.10.40 | FL-AS-01.PATCHLINK.COM | Windows 2003 Server | Agent Not Installed |
| 10.3.10.50 | FL-DC-01.PATCHLINK.COM | Windows 2003 Server EDC | Agent Not Installed |
| 10.3.10.58 | WINXPSP3-DC03 | Windows 2003 Server | Agent Not Installed |
| 10.3.10.60 | STLOUIS.PATCHLINK.COM | Windows 2003 Server | Agent Not Installed |

Figure 91: Composite Inventory Report

This following table describes each report field and column.

Table 99: Composite Inventory Report Field and Column Definitions

| Field / Column | Definition |
|---|---|
| **General Information** | |
| **Server Name** | The Lumension Endpoint Management and Security Suite server name. |
| **Agent Groups** | The agent groups included in the report. |
| **Job Name** | The job name. |
| **Date and Time Information** | |
| **Run Date** | The date the selected job ran. |
| **Start Time** | The time the selected job began. |
| **Duration** | The duration of the selected job. |
| **Version** | The version of the scan engine in use. |

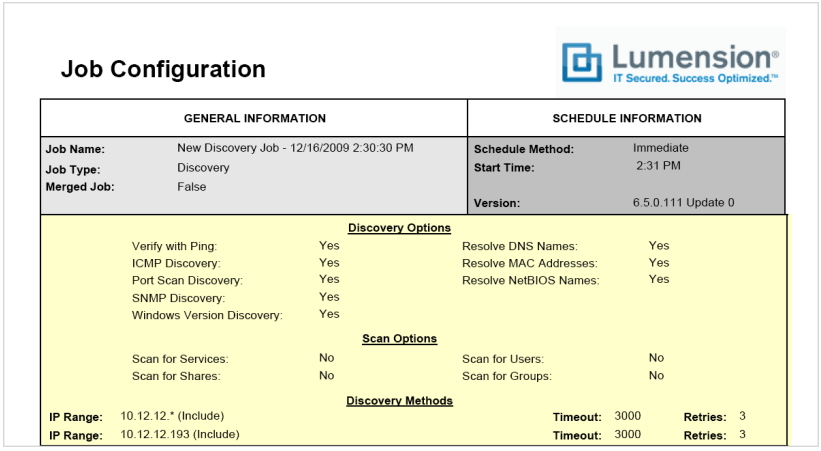
| Field / Column | Definition |
|---|---|
| **Endpoint Inventory Summary** | |
| **Total Known Endpoints** | The total number of endpoints with agents installed. |
| **Agents Checking In** | The number of agents checking in to the Lumension Endpoint Management and Security Suite. |
| **Online** | The total number/percentage of endpoints online. |
| **Agents Not Checking In** | The number of agents that are not checking in to Lumension Endpoint Management and Security Suite. |
| **Offline** | The number (or percentage) of agents that are offline. |
| **Disabled** | The number (or percentage) of agents that are disabled. |
| **No Agent Installed** | The number (or percentage) of endpoints with no agent installed. |
| **Not Installed** | The number (or percentage) of endpoints with no agent installed. |
| **Endpoint Inventory Summary Graph** | |
| **Disabled** | The number (or percentage) of agents that are disabled. |
| **Not Installed** | The number (or percentage) of endpoints with no agent installed. |
| **Offline** | The number (or percentage) of agents that are offline. |
| **Online** | The total number/percentage of endpoints online. |
| **Total** | The total number of endpoints assessed. |
| **Composite Inventory Table** | |
| **Agent IP** | The IP address of the endpoint the agent is installed on. |
| **Agent Name** | The name endpoint that hosts the agent. |
| **Operating System** | The operating system name and description. |
| **Agent Status** | The current status of the endpoint. |

### Job Configuration Report

This report comprehensively details a selected job's configuration. Use the ***Job Configuration*** report to document all configuration settings and options assigned to a selected job (discovery scan or agent management).

This report generates a listing of discovery options used by a specific job and can be used to maintain configuration control.

**Required Parameters**: Selection of one `completed job`.



Job Configuration

Lumension® IT Secured. Success Optimized.™

| GENERAL INFORMATION | | SCHEDULE INFORMATION | |
|---|---|---|---|
| **Job Name:** | New Discovery Job - 12/16/2009 2:30:30 PM | **Schedule Method:** | Immediate |
| **Job Type:** | Discovery | **Start Time:** | 2:31 PM |
| **Merged Job:** | False | **Version:** | 6.5.0.111 Update 0 |

**Discovery Options**

| | | | |
|---|---|---|---|
| Verify with Ping: | Yes | Resolve DNS Names: | Yes |
| ICMP Discovery: | Yes | Resolve MAC Addresses: | Yes |
| Port Scan Discovery: | Yes | Resolve NetBIOS Names: | Yes |
| SNMP Discovery: | Yes | | |
| Windows Version Discovery: | Yes | | |

**Scan Options**

| | | | |
|---|---|---|---|
| Scan for Services: | No | Scan for Users: | No |
| Scan for Shares: | No | Scan for Groups: | No |

**Discovery Methods**

| | | | | | |
|---|---|---|---|---|---|
| **IP Range:** | 10.12.12.* (Include) | **Timeout:** | 3000 | **Retries:** | 3 |
| **IP Range:** | 10.12.12.193 (Include) | **Timeout:** | 3000 | **Retries:** | 3 |

Figure 92: Job Configuration Report

The following table describes each report field.

Table 100: Job Configuration Report Field Definitions

| Field | Definition |
|---|---|
| **General Information** | |
| **Job Name** | The job name. |
| **Job Type** | The job type. |
| **Merged Job** | Indicates if the job is a merged job (`True` or `False`). |
| **Schedule Information** | |
| **Schedule Method** | The job schedule method. |
| **Start Time** | The time the selected job began. |
| **Version** | The version of the scan engine in use. |
| **Discovery Options** | |
| **Verify with Ping** | Indicates if the **Verify with Ping** discovery option was selected. |
| **ICMP Discovery** | Indicates if **ICMP Discovery** was selected. |
| **Port Scan Discovery** | Indicates if **Port Scan Discovery** was selected. |
| **SNMP Discovery** | Indicates if **SNMP Discovery** was selected. |

| Field | Definition |
|---|---|
| **Windows Version Discovery** | Indicates if **Windows Version Discovery** was selected. |
| **Resolve DNS Names** | Indicates if **Resolve DNS Names** was selected. |
| **Resolve MAC Addresses** | Indicates if **Resolve MAC Addresses** was selected. |
| **Resolve NetBIOS Names** | Indicates if **Resolve NetBIOS Names** was selected. |
| **Scan Options** | |
| **Scan for Services** | Indicates if the **Scan for Services** scan option was selected. |
| **Scan for Shares** | Indicates if **Scan for Shares** was selected. |
| **Scan for Users** | Indicates if **Scan for Users** was selected. |
| **Scan for Groups** | Indicates if **Scan for Groups** was selected. |
| **Discovery Methods** | |
| **IP Range** | Indicates a single IP address, wildcard IP address, or IP range designated for detection during a job. This field is associated with the **Single/Wildcard IP** and **IP Range** discovery methods. |
| **Machine Name** | Indicates the NetBIOS or DNS name of an endpoint designated for discovery during a job. This field is associated with the **Named Target** discovery method. |
| **Network Discovery** | Indicates a network neighborhood designated for discovery during a job. This field is associated with the **Network Neighborhood** discovery method. |
| **Credentials included in the credential set** | |
| **Credential Type** | The type of credentials entered during job configuration (`Windows`, `Posix`, `SNMP`). |
| **Description** | A description of the credentials used. |
| **User Name** | The user name entered during job credential configuration. This field is associated with `Windows` and `Posix` credentials. |
| **Community String** | The community string entered during job credential configuration. This field is associated with `SNMP` credentials. |

**Note:** The **Discovery Methods** and **Credentials included in the credential set** fields displayed depend on how the job was configured. For example, a report representing a job that did not use the **IP Range** discovery method will not display an **IP Range** field. Similarly, **Credential included in the credential set** fields are only populated if you entered credentials during job configuration.

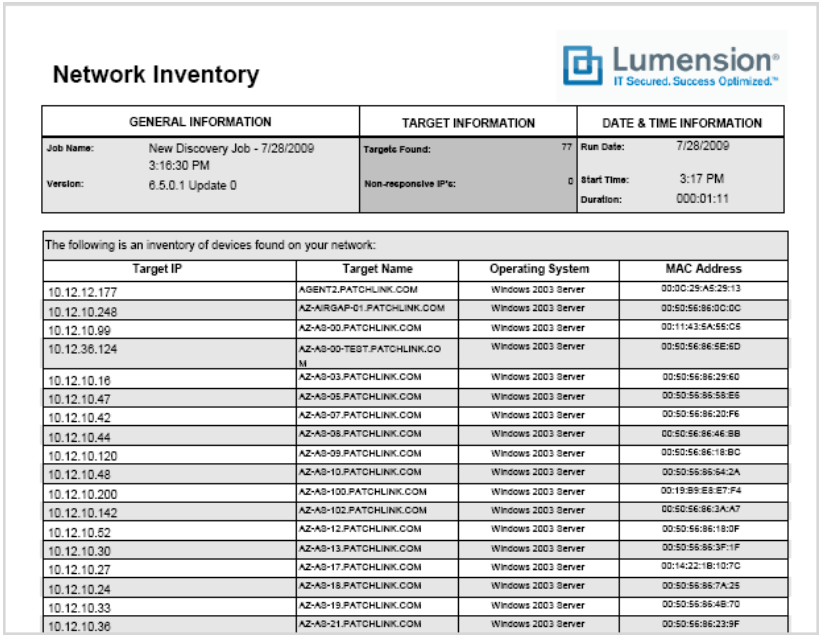
## Network Inventory Report

This report lists the endpoints, along with basic identification information, that were discovered during a job (discovery scan or agent management).

**Required Parameters**: Selection of one `completed job`.

**Optional Parameters**: `Sort by` (IP Address, Machine Name, Operating System [OS]), `Included OSs`, `Included IP adresses`.

**Note:** Enter a single IP or a range of IP addresses (leave blank for all).



Network Inventory

Lumension® IT Secured. Success Optimized.™

| GENERAL INFORMATION | | TARGET INFORMATION | | DATE & TIME INFORMATION | |
|---|---|---|---|---|---|
| Job Name: | New Discovery Job - 7/28/2009 3:16:30 PM | Targets Found: | 77 | Run Date: | 7/28/2009 |
| Version: | 6.5.0.1 Update 0 | Non-responsive IP's: | 0 | Start Time: | 3:17 PM |
| | | | | Duration: | 000:01:11 |

The following is an inventory of devices found on your network:

| Target IP | Target Name | Operating System | MAC Address |
|---|---|---|---|
| 10.12.12.177 | AGENT2.PATCHLINK.COM | Windows 2003 Server | 00:0C:29:A5:29:13 |
| 10.12.10.248 | AZ-AIRGAP-01.PATCHLINK.COM | Windows 2003 Server | 00:50:56:86:0C:0C |
| 10.12.10.99 | AZ-AS-00.PATCHLINK.COM | Windows 2003 Server | 00:11:43:5A:55:C5 |
| 10.12.36.124 | AZ-AS-00-TEST.PATCHLINK.COM | Windows 2003 Server | 00:50:56:86:5E:6D |
| 10.12.10.16 | AZ-AS-03.PATCHLINK.COM | Windows 2003 Server | 00:50:56:86:29:60 |
| 10.12.10.47 | AZ-AS-05.PATCHLINK.COM | Windows 2003 Server | 00:50:56:86:58:E6 |
| 10.12.10.42 | AZ-AS-07.PATCHLINK.COM | Windows 2003 Server | 00:50:56:86:20:F6 |
| 10.12.10.44 | AZ-AS-08.PATCHLINK.COM | Windows 2003 Server | 00:50:56:86:46:BB |
| 10.12.10.120 | AZ-AS-09.PATCHLINK.COM | Windows 2003 Server | 00:50:56:86:18:BC |
| 10.12.10.48 | AZ-AS-10.PATCHLINK.COM | Windows 2003 Server | 00:50:56:86:64:2A |
| 10.12.10.200 | AZ-AS-100.PATCHLINK.COM | Windows 2003 Server | 00:19:B9:E8:E7:F4 |
| 10.12.10.142 | AZ-AS-102.PATCHLINK.COM | Windows 2003 Server | 00:50:56:86:3A:A7 |
| 10.12.10.52 | AZ-AS-12.PATCHLINK.COM | Windows 2003 Server | 00:50:56:86:18:0F |
| 10.12.10.30 | AZ-AS-13.PATCHLINK.COM | Windows 2003 Server | 00:50:56:86:3F:1F |
| 10.12.10.27 | AZ-AS-17.PATCHLINK.COM | Windows 2003 Server | 00:14:22:1B:10:7C |
| 10.12.10.24 | AZ-AS-18.PATCHLINK.COM | Windows 2003 Server | 00:50:56:86:7A:25 |
| 10.12.10.33 | AZ-AS-19.PATCHLINK.COM | Windows 2003 Server | 00:50:56:86:4B:70 |
| 10.12.10.36 | AZ-AS-21.PATCHLINK.COM | Windows 2003 Server | 00:50:56:86:23:9F |

Figure 93: Network Inventory Report

The following table describes the report field and columns.

Table 101: Network Inventory Report Field and Column Definitions

| Field / Column | Definition |
|---|---|
| **General Information** | |
| **Job Name** | The job name. |
| **Version** | The version of the scan engine in use. |
| **Target Information** | |
| **Targets Found** | The number of endpoints discovered during scanning. |
| **Non-responsive IP's** | The number of IP addresses designated for discovery during job configuration that were unresponsive. |

| Field / Column | Definition |
|---|---|
| **Date and Time Information** | |
| **Run Date** | The date the selected job ran. |
| **Start Time** | The time the selected job began. |
| **Duration** | The duration of the selected job. |
| **Network Inventory Table Columns** | |
| **Target IP** | The IP address of the discovered endpoint. |
| **Target Name** | The DNS name of the endpoint. |
| **Operating System** | The operating system name and description. |
| **MAC Address** | The MAC address of the endpoint. |

# Chapter 11

# Managing Lumension EMSS Users and Roles

**In this chapter:**


- The Users and Roles Page
- The Users Tab
- Working with Users
- The Roles Tab
- Working with Roles


User and role management features let you add, edit, and delete Lumension Endpoint Management and Security Suite users, and also assign users access rights.

Create, configure, and manage users and roles from the ***Users and Roles*** page.

## The Users and Roles Page

This page lets you create users and user roles for user withing Lumension Endpoint Management and Security Suite (Lumension EMSS). *Users* are a name or title used to log in to the Lumension EMSS Web console, while *user roles* are sets of access rights, accessible groups, and accessible endpoints assigned to users that determine what functions and pages are available.

Existing users and user roles are listed on their respective tabs.

The ***Users and Roles*** page contains the following tabs:

- *The Users Tab* on page 251
- *The Roles Tab* on page 262

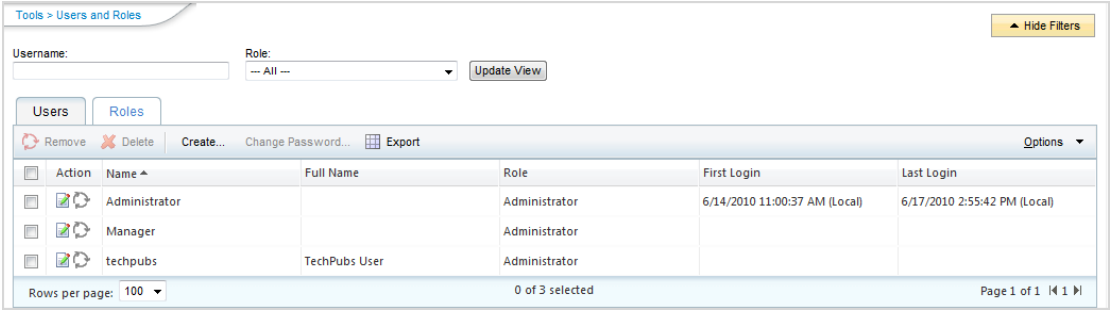



Figure 94: Users and Roles Page

## Viewing the Users and Roles Page

Navigate to this page to create and manage users and user roles.

You can access this page at any time using the navigation menu.

1. Select **Tools** > **Users and Roles**.
2. Select a tab based on the task you want to accomplish:
   - To work with users, select the **Users** tab.
   - To work with roles, select the **Roles** tab.
3. If desired, complete a task.
   - To complete a task related to users, perform a task listed in *Working with Users* on page 253.
   - To complete a task related to roles, perform a task listed in *Working with Roles* on page 269.

## Defining User Access

Lumension Endpoint Management and Security Suite (Lumension EMSS) supports the establishment of security policies that conform to your network needs. Two mechanisms determine security access: Windows-based authentication and Lumension EMSS access rights.

### Windows-Based Authentication

Lumension EMSS authentication is controlled by the Windows operating system. Users who have access to Lumension EMSS are members of the local Windows group `PLUS Admins`.

### Lumension EMSS Access Rights

After a user logs in to Lumension EMSS, the system authenticates the user's assigned role. If a user does not have access to a given Lumension EMSS page or function, an access denied message displays, or the feature is simply unavailable.

On the ***Users and Roles*** page, the ***Roles*** tab is where roles are defined, while the ***Users*** tab is where you can add or remove users and assign them a role.

# The Users Tab

This tab lets you create and manage *users*.

Additionally, you can use this tab to edit users, remove users, or assign them user roles.

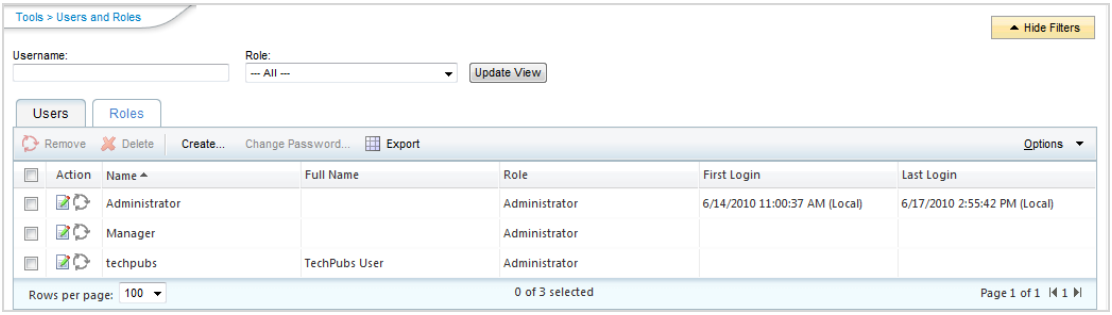



Figure 95: Users Tab

## Defining Users

*Users* are names or titles that people use to access Lumension Endpoint Management and Security Suite (Lumension EMSS). Users can be defined as individuals (John Smith) or conceptual users (Quality Assurance Manager). The user profile includes access credentials (user name and password) and the role assigned to the user. A user can be assigned only one role, and many users can share one role.

There are two methods of introducing users to the system: creating users and adding users.

| | |
|---|---|
| **Creating New Users** | When a user is created, that user is added to both Lumension EMSS and Windows. Additionally, new users assigned the **Manage Users** access right are added to the Windows Administrators group; without addition to this group, the user would be unable to modify other users. |
| **Adding Existing Windows Users** | You can grant existing Windows users (both local users and domain users) access to Lumension EMSS. Using this method, you can search Windows for existing users and add them to Lumension EMSS. Additionally, added users assigned the **Manage Users** access right are added to the Windows Administrators group; without addition to this group, the user would be unable to modify other users. |

**Note:** Microsoft IIS Web server software, used by Lumension EMSS, does not support user names or passwords in languages that require unicode characters (such as Korean or Kanji).

## The Users Tab Toolbar

This toolbar contains buttons that let you create and manage users.

The following table describes the function of each toolbar button.

Table 102: Users Tab Toolbar

| Button | Function |
|---|---|
| **Remove** | Removes the selected user. For additional information, refer to *Removing Lumension EMSS Users* on page 258. |
| **Delete** | Deletes the selected user. For additional information, refer to *Deleting Lumension EMSS Users* on page 259. |
| **Create...** | Creates a new user. For additional information, refer to *Creating New Lumension EMSS Users* on page 253. |
| **Change Password...** | Changes the password for the selected user. For additional information, refer to *Changing a User Password* on page 259. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |
| **Options** (menu) | Opens the **Options** menu. For additional information, refer to *The Options Menu* on page 31. |

## The Users Tab List

This list displays each user role within the system. Use the list icons to edit or remove users. Additionally, you can also filter the lists to display only specified roles.

The following table describes the ***Users*** tab list columns.

Table 103: Users Tab List

| Column | Description |
|---|---|
| **Action** | Contains **Edit** and **Remove** icons. Use these icons to edit or remove the associated user. For additional information, refer to one of the following topics:<br>• *Editing Lumension EMSS Users* on page 257<br>• *Removing Lumension EMSS Users* on page 258 |
| **Name** | The Lumension Endpoint Management and Security Suite user name. |
| **Full Name** | The full name of the user. |

| Column | Description |
|---|---|
| **Role** | The role assigned to the user. |
| **First Login** | The date and time of the first time the user logged in. |
| **Last Login** | The date and time of the last time the user logged in. |

## Working with Users

To perform tasks associated with users, click a toolbar button or list icon. To perform some tasks, selecting one or multiple users from the list may be necessary.


- *Creating New Lumension EMSS Users* on page 253
- *Adding Existing Windows Users to Lumension EMSS* on page 255
- *Editing Lumension EMSS Users* on page 257
- *Removing Lumension EMSS Users* on page 258
- *Deleting Lumension EMSS Users* on page 259
- *Changing a User Password* on page 259
- *Changing Your Password* on page 260
- *Exporting User Data* on page 261


### Creating New Lumension EMSS Users

Create a new Lumension Endpoint Management and Security Suite (Lumension EMSS) user when you need to allow a person within your organization access to Lumension EMSS. New users are added to both Lumension EMSS and Windows.

Create new users from the ***Users*** tab.

1. Select **Tools** > **Users and Roles**.
2. Ensure the ***Users*** tab is selected.

3. Click **Create...**.

   **Step Result:** The ***Create User Wizard*** opens.

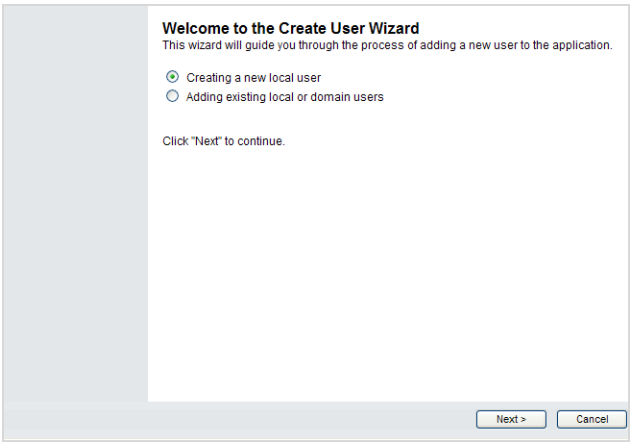

Welcome to the Create User Wizard
This wizard will guide you through the process of adding a new user to the application.
Creating a new local user
Adding existing local or domain users
Click "Next" to continue.
Next >
Cancel

Figure 96: Creating a New Local User

4. Select the **Creating a new local user** option.
5. Click **Next**.
6. Define the user credentials.

   Type the applicable information in the following fields.

| Field Name | Description |
|---|---|
| **User name** | The desired user name.<br>**Note:** The **User Name** must be 1-20 characters in length and cannot include any of the following characters:<br>• ‘ \ “ @ ^ % & { } ( ) [ ] ; < > ! # : ? / = \| |
| **Password** | The desired password.<br>The **Password Strength** indicator factors password effectiveness based on password length, complexity, character variety, and common word resemblance.<br>Strong passwords contain eight characters or greater and combine symbols, numbers, uppercase letters, and lowercase letters. Also, they do not resemble common words or names, including words with numbers in place of letters. |
| **Confirm Password** | The password retyped. |

7. From the **Role** list, select the desired role.

   Select from the following roles:

   - **Administrator**
   - **Manager**
   - **Operator**
   - **Guest**
   - ***Custom Role(s)***

   **Note:** ***Custom Role(s)*** are only available if a custom role has been created.

8. If desired, define the user information.

   Type the applicable information in the remaining fields.

| Field Name | Description |
|---|---|
| **Description** | The description of the user. |
| **Full name** | The full name of the user. |
| **Office phone** | The office phone number of the user. |
| **Cell phone** | The cell phone number of the user. |
| **Pager** | The pager number of the user. |
| **E-mail** | The e-mail address of the user. |

9. Click **Finish**.
10. Click **Close**.

**Result:** The ***Create User Wizard*** closes and the user is created. The new user can now access all authorized features of Lumension EMSS. Lumension EMSS administrators can edit the user from the ***Users*** tab.

## Adding Existing Windows Users to Lumension EMSS

When you want to add a pre-existing Windows domain or local user as a user within Lumension Endpoint Management and Security Suite (Lumension EMSS), you can add that user instead of creating a new one. Import a user from an existing domain by logging into that domain as a domain user.

Add existing Windows users from the ***Users*** tab.

1. Select **Tools** > **Users and Roles**.
2. Ensure the ***Users*** tab is selected.

3. Click **Create...**.

   **Step Result:** The ***Create User Wizard*** opens.

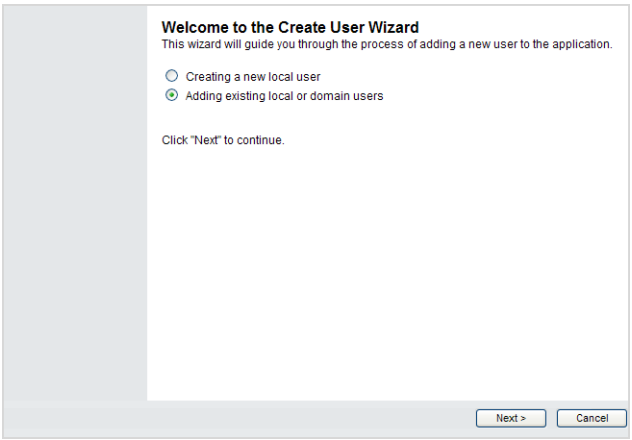

Welcome to the Create User Wizard
This wizard will guide you through the process of adding a new user to the application.
Creating a new local user
Adding existing local or domain users
Click "Next" to continue.
Next >
Cancel

Figure 97: Adding Existing Local or Domain Users

4. Select the **Adding existing local or domain users** option.
5. Click **Next**.
6. In the **Search for the following users** field, type a user name, or the beginning characters of one or more user names. Use semicolons to separate user names.

   To search for users within a specific domain, prefix the user name with the domain (*DOMAINNAME\UserName*).

   **Note:** There must be a secure connection between the domain and the Lumension EMSS's domain, or the user will be unable to access Lumension EMSS.

7. Click **Next.**
8. From the **Role** list, select the desired role.

   Select from the following roles:

   - **Administrator**
   - **Manager**
   - **Operator**
   - **Guest**
   - ***Custom Role(s)***

   **Note:** ***Custom Role(s)*** are only available if a custom role has been created.

9. Click **Finish**.
10. Click **Close**.

**Result:** The ***Create User Wizard*** closes and the user is added. The added Windows user can now access Lumension EMSS and all authorized features.

## Editing Lumension EMSS Users

Edit existing Lumension Endpoint Management and Security Suite users to change their assigned role(s) or contact information.

Edit users from the ***Users*** tab.

1. Select **Tools** > **Users and Roles**.
2. Ensure the ***Users*** tab is selected.
3. Click the **Edit** icon associated with the user you want to edit.

   **Step Result:** The ***Edit User*** dialog opens.

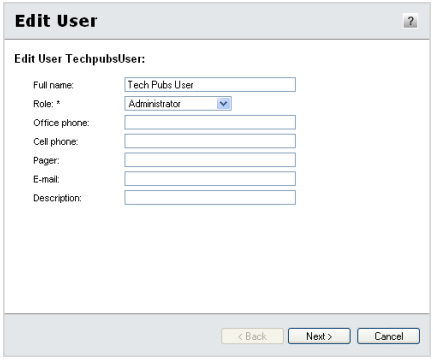



Figure 98: Edit User Dialog

4. If desired, edit the **Full name** field.
5. If desired, select a new role from the **Role** list.

   Select one of the following roles:

   - **Administrator**
   - **Manager**
   - **Operator**
   - **Guest**
   - ***Custom Role(s)***

**Note:** *Custom Role(s)* are only available if a custom role has been created.

6. If desired, edit the following fields.

| Field Name | Description |
|---|---|
| **Office phone** | The user's office phone number. |
| **Cell phone** | The user's cell phone number. |
| **Pager** | The user's pager number. |

| Field Name | Description |
|---|---|
| **E-mail** | The user's email address. |
| **Description** | The user's description. |

7. Click **Next**.
8. Click **Finish**.

**Result:** The user is updated according to your changes.

## Removing Lumension EMSS Users

Removing a user account removes it from Lumension Endpoint Management and Security Suite (Lumension EMSS) without deleting that user account within Windows or on Active Directory. Remove users when you no longer want them to have access to Lumension EMSS yet still want their user accounts to exist.

Once removed, the user is removed from the Lumension EMSS endpoint groups and the user list on the ***Users and Roles*** page. Remove users from the ***Users*** tab.

**Note:** You cannot remove users assigned the **Administrator** role. You must first edit the user, change the role, then remove the user.

1. Select **Tools** > **Users and Roles**.
2. Ensure the ***Users*** tab is selected.
3. Remove the desired user(s).

   Use one of the following methods.

| Method | Steps |
|---|---|
| **To remove a single user:** | Click the **Remove** icon associated with the user you want to remove. |
| **To remove multiple users:** | 1. Select the check boxes associated with the users you want to remove.<br>2. From the toolbar, click the **Remove** button. |

   **Step Result:** A dialog displays, asking you to acknowledge the removal.

4. Acknowledge the removal by clicking **OK**.

**Result:** The user is removed from Lumension EMSS. You can re-add the removed user at any time if the user's Windows account still exists.

## Deleting Lumension EMSS Users

Delete a Lumension Endpoint Management and Security Suite (Lumension EMSS) user when you want to remove it from both Lumension EMSS and Windows. Deleting users removes them from Lumension EMSS and Windows (locally), whereas removing users only removes them from Lumension EMSS.

Delete users from the ***Users and Roles*** page ***Users*** tab.

**Note:** You cannot delete users assigned the **Administrator** role. You must first edit the user, change the role, then remove the user.

1. Select **Tools** > **User and Roles**.
2. Ensure the ***Users*** tab is selected.
3. Select the check box(es) associated with the user(s) you want to delete.
4. Click **Delete**.

   **Caution:** Deleting a user deletes them from both Lumension EMSS and Windows (locally).

   **Step Result:** A dialog displays, asking you to acknowledge the deletion.

5. Acknowledge the deletion by clicking **OK**.

**Result:** The user is deleted from both Lumension EMSS and Windows (locally).

**Note:** Deleting a Lumension EMSS user that was added from your Active Directory will not delete the Windows user account within Active Directory. The account will only be removed from Lumension EMSS.

## Changing a User Password

If you have the **Change Password** access right, you can edit other user's passwords. Changing a user's password in Lumension Endpoint Management and Security Suite also changes the user's Windows password on the Lumension Endpoint Management and Security Suite server or Active Directory. Change a password for security reasons or if a user has forgotten theirs.

Change user passwords from the ***Users*** tab.

1. Select **Tools** > **Users and Roles**.
2. Ensure the ***Users*** tab is selected.
3. Select the check box associated with the user whose password you want to change.
4. Click **Change Password...**.

   **Step Result:** The ***Change password for*** dialog opens.

5. Type a new password in the **New Password** field.

   The **Password Strength** indicator factors your password security based on length, complexity, character variety, and common word resemblance.

Strong passwords contain eight characters or greater and combine symbols, numbers, and letters (both upper and lowercase). Also, they do not resemble common words or names, including words with numbers in place of letters.

**Attention:** Passwords must adhere to Windows local and/or domain password policies.

Figure 99: Change My Password Dialog

6. Retype the password in the **Confirm Password** field.
7. Click **Finish**.

**Result:** The password is changed.

## Changing Your Password

You can change your own password at any time. Changing your password in Lumension Endpoint Management and Security Suite (Lumension EMSS) also changes your Windows password on the Lumension EMSS server or Active Directory.

Change your password from the navigation menu.

1. Select **Tools** > **Change My Password...**.

   **Step Result:** The ***Change My Password*** dialog opens.

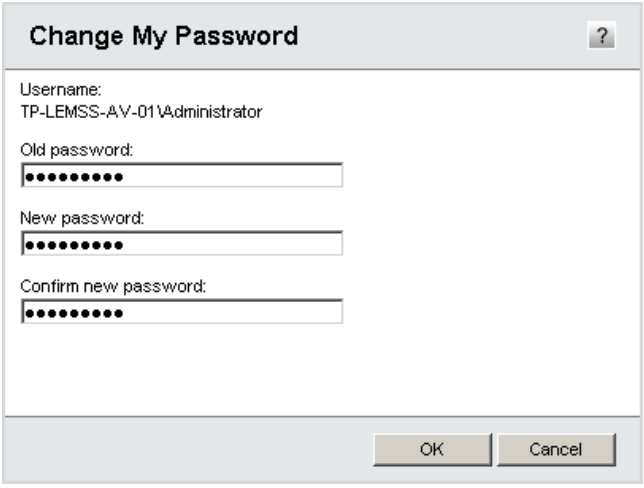



Figure 100: Change My Password Dialog

2. Type your old password in the **Old password** field.

   The **Password Strength** indicator factors password effectiveness based on password length, complexity, character variety, and common word resemblance.

   Strong passwords contain eight characters or greater and combine symbols, numbers, uppercase letters, and lowercase letters. Also, they do not resemble common words or names, including words with numbers in place of letters.

   **Attention:** Passwords must adhere to Windows local and/or domain password policies.

3. Type your new password in the **New Password** field.
4. Retype your new password in the **Confirm New Password** field.
5. Click **OK**.

**Result:** Your password is changed. Use your new password the next time you log in to Lumension EMSS, Windows, or Active Directory.

## Exporting User Data

You can export the data displayed on the ***Users*** tab list so that it can be used in other applications. This data is exported to a comma separated value (`.csv`) file.

To export data, click the **Export** button. For additional information, refer to *Exporting Data* on page 37.

# The Roles Tab

This tab lets you create new user roles and manage existing user roles.

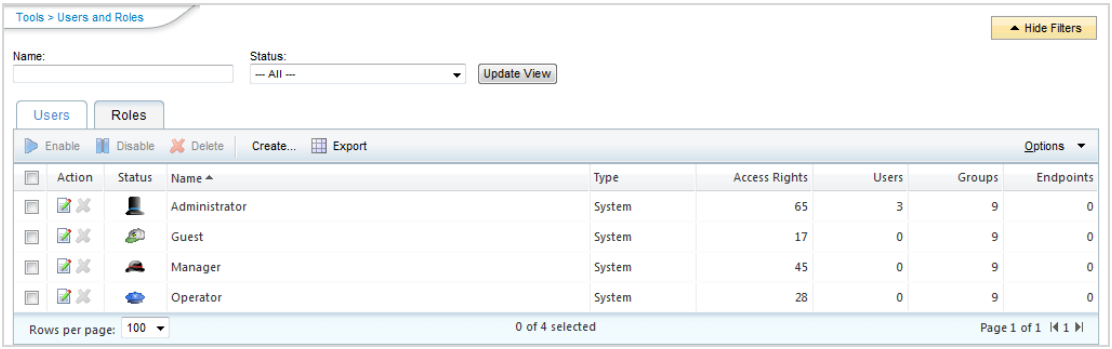



Figure 101: Roles Tab

## Defining Roles

*User Roles* are assignable sets of access rights, accessible groups, and accessible endpoints that determine what functions and pages are available to Lumension Endpoint Management and Security Suite (Lumension EMSS) users. Roles can be customized and assigned to various users.

Lumension EMSS uses two types of roles: system roles and custom roles.

| | |
|---|---|
| ***System Roles*** | These roles are included with the default Lumension EMSS installation. These roles are predefined with access rights appropriate for various users. System roles cannot be edited or disabled, and they can access all system groups and endpoints. |
| ***Custom Roles*** | These roles are created after Lumension EMSS installation by users with the **Manage Users** access right. Custom roles let you grant users unique sets of access rights. Additionally, these roles let you define specific endpoints and groups that can be accessed and managed. |

Roles are defined by a combination of three attributes: access rights, accessible groups, and accessible endpoints.

Table 104: Role Attribute Descriptions

| Role Attribute | Description |
|---|---|
| Access Rights | Define the pages and functions available to the user. |
| Accessible Groups | Define the specific endpoint groups accessible to the user. |
| Accessible Endpoints | Define the specific endpoints accessible to the user. |

### Predefined System Roles

Predefined system roles are the default roles offered by Lumension Endpoint Management and Security Suite (Lumension EMSS). The commonly used access rights selected for these roles are usually adequate for most

networks and their users. Additionally, these roles can access and manage all Lumension EMSS groups and endpoints.

These roles assist you in assigning commonly used access rights to new users. Users with the **Manage Users** access rights can assign these system roles to a user, or use them as templates for creating a custom role. The following table describes the predefined system roles and the icons that denote them.

Table 105: Predefined System Role Descriptions

| Role | Icon | Description |
|---|---|---|
| **Administrator** | | Users have full access to all Lumension EMSS pages and functions. Administrators are the only users who can delegate newly installed endpoints to other user roles. The administrator role includes all access rights. At least one user must be assigned the administrator role at all times. |
| **Guest** | | Users can access various Lumension EMSS pages, but cannot use their functions; this role allows read-only access. |
| **Manager** | | Users can access most Lumension EMSS pages and functions. |
| **Operator** | | Users can perform all routine functions (detect, export, and so on). Operators can only perform typical daily functions. |

**Note:** A user assigned a system role has access to all endpoints and groups.

### Custom Roles

Custom roles are user roles that only have the user access rights, accessible groups, and accessible endpoints you select. Create custom roles for users who require unique sets of access rights.

Custom roles are created by users with the **Manage Users** access right. Preexisting roles can be used as templates when creating custom roles. Additionally, you can configure a custom group to restrict users to management of specific groups and endpoints. Finally, unlike system roles (which cannot be disabled or deleted), you can disable or delete a custom role at any time. Custom roles are denoted by the **Wool Hat** icon.

## Defining Access Rights

*Access rights* are individual privileges that define whether a user can access a system feature. These rights control availability for every Lumension Endpoint Management and Security Suite (Lumension EMSS) page, feature, function, and action. The pages and features available to users are based on the access rights associated with the role assigned to them. The system roles are assigned a default set of access rights. Users inherit the access rights of the role they are assigned.

Access rights begin with read-only access to system pages and permission to export data. At the administrative level, users can be assigned rights to fully manage the various system pages and functions. These functions include deployment initiation, user and role creation, and so on.

**Note:** If a software expansion is installed with Lumension EMSS, access rights for the expansion may be added to the access rights list.

The following table identifies and describes the default set of access rights for each system role: **Administrator** (Admin.), **Manager** (Man.), **Operator** (Op.), and **Guest**.

Table 106: User Role Access Rights

| Access Right | Description | Admin. | Man. | Op. | Guest |
|---|---|---|---|---|---|
| Dashboard | | | | | |
| **View Dashboard** | Access to view the ***Home*** page dashboard. | X | X | X | X |
| **View Current Status** | Access to view the status of the server. | X | X | X | X |
| Jobs | | | | | |
| **View Discovery Scan Jobs** | Access to view discovery scan jobs. | X | X | | |
| **Create Discovery Scan Jobs** | Access to create and copy discovery scan jobs. | X | X | | |
| **View Agent Management Jobs** | Access to view agent management jobs. | X | X | | |
| **Create Agent Management Jobs** | Access to create and copy agent management jobs. | X | X | | |
| **Manage Modules via Jobs** | Access to install or uninstall agent modules via agent management jobs. | X | X | | |
| **Manage Jobs** | Cancel, pause, resume, deleted, or merge all jobs the user has access to. | X | X | | |
| **Export Jobs** | Export the jobs list. | X | X | | |
| Endpoints | | | | | |
| **View Endpoints** | Access the manage endpoints ***All*** tab and endpoint details. | X | X | X | X |
| **Manage All Tab** | Enable and disable agents, delete endpoints, and change agent versions. | X | X | | |
| **Export All Tab** | Export the ***All*** tab endpoints list. | X | X | X | |
| **Download Agent Installers** | Access the ***Download Agent Installer*** page. | X | X | X | |
| Groups | | | | | |
| **View Groups** | Access the groups. | X | X | X | X |
| **Manage Groups** | Add, edit, enable, disable, and delete groups. | X | X | | |

| Access Right | Description | Admin. | Man. | Op. | Guest |
|---|---|---|---|---|---|
| **Export Groups** | Export the groups. | X | X | X | |
| Users | | | | | |
| **View Users** | Access the users and roles. | X | X | X | X |
| **Manage Users** | Create, delete, enable, and disable users and roles. | X | | | |
| **Export Users** | Export the users and roles data. | X | X | | |
| Agent Policy Sets | | | | | |
| **View All Agent Policy Sets** | Access the agent policy sets. | X | X | X | X |
| **Manage All Agent Policy Sets** | Create, edit, and delete agent policy sets. | X | | | |
| **Export All Agent Policy Sets** | Export the agent policy sets list. | X | X | | |
| Reports | | | | | |
| **Reports Administrator** | Generate application reports regardless of access rights. | X | | | |
| **View My Core Reports** | Generate core reports only for those items this user has access to. | X | X | X | X |
| **Export Reports** | Export the generated reports. | X | X | X | |
| Manage Server Modules | | | | | |
| **Installation Manager** | Access to the Installation Manager to install, update, and uninstall server modules. | X | | | |
| Subscriptions | | | | | |
| **View Subscription** | Access the subscription information. | X | X | X | X |
| **Manage Subscription** | Edit or update subscription service updates. | X | | | |
| **Export Subscription** | Export the subscription information. | X | X | X | |
| Email Notifications | | | | | |
| **View Email Notifications** | Access the email notifications. | X | X | X | X |
| **Manage Email Notifications** | Create and edit email notifications and settings. | X | | | |

| Access Right | Description | Admin. | Man. | Op. | Guest |
|---|---|---|---|---|---|
| **Export Email Notifications** | Export the email notifications. | X | X | | |
| Options | | | | | |
| **View Options** | Access to general, agent, and deployment default server options. | X | X | X | X |
| **Manage Options** | Set and edit general, agent, and deployment default server options. | X | | | |
| **Export Options** | Export the **Options** list. | X | | | |
| Technical Support | | | | | |
| **View Technical Support** | Access the technical product support information. | X | X | X | X |
| **Export Technical Support** | Export the technical product support information. | X | X | X | |
| Licenses | | | | | |
| **View Licenses** | Access the product licenses. | X | X | X | X |
| **Manage Licenses** | Update product licenses. | X | | | |
| **Export Licenses** | Export the product licenses. | X | X | | |

## Defining Accessible Groups

*Accessible groups* are specific groups of endpoints that a particular role can access and manage. Use this feature for granularity when assigning roles to users.

Accessible groups are only applicable to custom user roles.

**Note:** The **Accessible Groups** feature is disabled when working with a predefined system role. System roles can access all groups and endpoints within the system.

This feature allows you to restrict a user to specified groups. For example, a user assigned the access right to manage deployments can be limited to managing deployments for select groups.

The **Accessible Groups** feature is defined on the ***Groups*** tab in both the ***Create Role*** dialog and the ***Edit Role*** dialog.

The ***Groups*** tab contains the following lists, which are used to control what groups are associated with a particular role:

Table 107: Groups Tab List Descriptions

| List | Description |
|---|---|
| Selected Groups | Lists the groups assigned to the role. |

| List | Description |
|---|---|
| Available Groups | Lists the available groups that can be assigned to the role. |

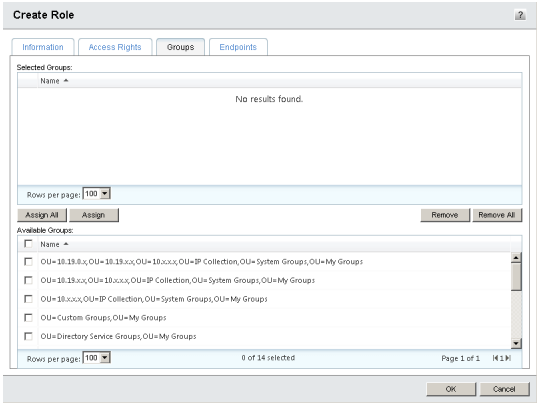



Figure 102: Roles Dialog Group Tab

## Defining Accessible Endpoints

*Accessible Endpoints* are specific endpoints that a particular role can access and manage. This feature is similar to the **Accessible Groups** feature; it allows for granularity when assigning roles to system users.

Accessible endpoints are only applicable to custom user roles.

**Note:** The **Accessible Endpoints** feature is disabled when working with predefined system roles. System roles can access all groups and endpoints within the system.

As mentioned, this feature lets you define specific endpoints that users associated with the role can access and manage. For example, you can limit a user assigned the **Manage Endpoints** access right to management of a single endpoint.

This feature is are defined on the ***Endpoints*** tab in both the ***Create Role*** dialog and the ***Edit Role*** dialog.

The ***Endpoints*** tab contains the following lists, which are used to control which endpoints are associated with a role:

Table 108: Endpoint Tab List Descriptions

| List | Description |
|---|---|
| Selected Endpoints | Lists the endpoints assigned to the role. |

| List | Description |
|---|---|
| Available Endpoints | Lists the available endpoints that can be assigned to the role. |

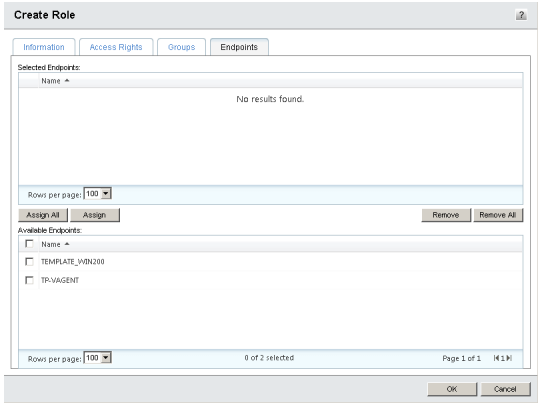



Figure 103: Roles Dialog Endpoints Tab

## The Roles Tab Toolbar

This toolbar contains buttons that let you create and manage user roles.

The following table describes the function of each ***Roles*** tab toolbar button.

Table 109: Roles Tab Toolbar

| Button Name | Function |
|---|---|
| **Enable** | Enables the selected disabled custom role. For additional information, refer to *Enabling User Roles* on page 273. |
| **Disable** | Disables the selected custom role. For additional information, refer to *Disabling User Roles* on page 273. |
| **Delete** | Deletes the selected custom role. For additional information, refer to *Deleting User Roles* on page 273. |
| **Create...** | Creates a new user role. For additional information, refer to *Creating User Roles* on page 270. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |

| Button Name | Function |
|---|---|
| **Options** (menu) | Opens the **Options** menu. For additional information, refer to *The Options Menu* on page 31. |

### The Roles Tab List

This list displays all user roles that exist within Lumension Endpoint Management and Security Suite. Use the action icons to manage roles. Additionally, this list can be filtered to display only specified roles.

The following table describes each ***Roles*** tab list column.

Table 110: Roles Tab List

| Column | Description |
|---|---|
| **Action** | Contains **Edit** and **Delete** icons. Use these icons to edit or delete the associated role. For addition information, refer to one of the following topics:<br>• *Editing User Roles* on page 271<br>• *Deleting User Roles* on page 273 |
| **Status** | Contains an icon that indicates the type of role. For additional information, refer to one of the following topics:<br>• *Predefined System Roles* on page 262<br>• *Custom Roles* on page 263 |
| **Name** | The name of the user role. |
| **Type** | The type of user role (`System` or `Custom`). |
| **Access Rights** | The number of access rights assigned to the role. |
| **Users** | The number of users assigned to the role. |
| **Groups** | The number of accessible groups assigned to the role. |
| **Endpoints** | The number of accessible endpoints assigned to the role. |

## Working with Roles

To perform tasks associated with roles, click a toolbar button or a list icon. To perform some tasks, selecting one or multiple roles from the list may be necessary.

- *Creating User Roles* on page 270
- *Editing User Roles* on page 271
- *Disabling User Roles* on page 273
- *Enabling User Roles* on page 273
- *Deleting User Roles* on page 273
- *Exporting User Role Data* on page 274

## Creating User Roles

Custom roles let you select individual access rights, accessible groups, and accessible endpoints for that role. Create a custom role when predefined system roles do not contain the access rights needed for a particular user. Creating a custom role is also useful when you require a role that can only access specific groups or endpoints.

Create custom roles from the ***Roles*** tab.

1. Select **Tools** > **Users and Roles**.
2. Select the ***Roles*** tab.
3. Click **Create...**.

   **Step Result:** The ***Create Role*** dialog opens to the ***Information*** tab.
4. Type a name in the **Name** field.
5. Type a description in the **Description** field.
6. Select a role template from the **Role Template** list.

   Any existing role can be used as a template. The selected role determines initial access rights. You can later change which access rights are assigned to the role.
7. Select the ***Access Rights*** tab.
8. Select or clear the desired access rights.

   For additional information, refer to *Predefined System Roles* on page 262.

   **Tip:** Select or clear the **All** check box to globally select or clear all access rights. Additionally, child access rights are unavailable until their parent access rights are selected.
9. Select the ***Groups*** tab.
10. Assign the desired accessible endpoint groups to the role.

    Use one of the following methods to assign groups.

| Method | Steps |
|---|---|
| **To assign individual groups:** | 1. From the **Available Groups** table, select the check box(es) associated with the group(s) you want to assign.<br>2. Click **Assign**. |
| **To assign all groups:** | Click **Assign All**. |

    **Tip:** Remove groups using **Remove** and **Remove All**.
11. Select the ***Endpoints*** tab.

12. Assign the desired accessible endpoints to the role.

    Use one of the following methods to assign endpoints.

| Method | Steps |
|---|---|
| **To assign individual endpoints:** | 1. From the **Available Endpoints** table, select the check box(es) associated with the endpoint(s) you want to assign.<br>2. Click **Assign**. |
| **To assign all endpoints:** | Click **Assign All**. |

**Tip:** Remove endpoints using **Remove** and **Remove All**.

13. Click **OK**.

**Result:** Your new role is saved. It can now be assigned to users. Additionally, it can be edited from the ***Users and Roles*** page **Roles** tab.

## Editing User Roles

Edit a custom user role as the needs of users associated with the role change. You can only edit custom roles (predefined system roles cannot be edited).

Edit roles from the ***Roles*** tab.

1. Select **Tools** > **User and Roles**.
2. Select the ***Roles*** tab.
3. Click the **Edit** icon associated with the role you want to edit.

   **Step Result:** The ***Edit Role*** dialog opens to the ***Information*** tab.
4. If desired, edit the **Description** field.
5. If desired, select a role template from the **Role Template** list.

   Any existing role can be used as a template. The selected role determines initial access rights. You can later change which access rights are assigned to the role.
6. Select the ***Access Rights*** tab.
7. If desired, select or clear the desired access rights.

**Tip:** Select or clear the **All** check box to globally select or clear all access rights. Additionally, child access rights are unavailable until their parent access rights are selected.

8. Select the ***Groups*** tab.

9. If desired, assign accessible endpoint groups to the role.
   Use one of the following methods to assign groups.

| Method | Steps |
|---|---|
| **To assign individual groups:** | 1. From the **Available Groups** table, select the check box(es) associated with the group(s) you want to assign.<br>2. Click **Assign**. |
| **To assign all groups:** | Click **Assign All**. |

10. If desired, remove accessible endpoint groups from the role.
    Use one of the following methods to remove groups.

| Method | Steps |
|---|---|
| **To remove individual groups:** | 1. From the **Selected Groups** table, select the check box(es) associated with the group(s) you want to remove.<br>2. Click **Remove**. |
| **To remove all groups:** | Click **Remove All**. |

11. Select the ***Endpoints*** tab.
12. If desired, assign accessible endpoints to the role.
    Use one of the following methods to assign endpoints.

| Method | Steps |
|---|---|
| **To assign individual endpoints:** | 1. From the **Available Endpoints** table, select the check box(es) associated with the endpoint(s) you want to assign.<br>2. Click **Assign**. |
| **To assign all endpoints:** | Click **Assign All**. |

13. If desired, remove accessible endpoints from the role.
    Use one of the following methods to remove endpoints.

| Method | Steps |
|---|---|
| **To remove individual endpoints:** | 1. From the **Selected Endpoints** table, select the check box(es) associated with the endpoint(s) you want to remove.<br>2. Click **Remove**. |

| Method | Steps |
|---|---|
| **To remove all endpoints:** | Click **Remove All**. |

14. Click **OK**.

**Result:** Your edits are saved. The edited role is applied to all associated users.

## Disabling User Roles

You can disable any custom role, allowing you to maintain the role within Lumension Endpoint Management and Security Suite without assigning it to users. You can enable, edit, and delete disabled roles. Disabled roles appear unavailable.

Disable roles from the ***Roles*** tab.

**Note:** You cannot disable system roles: **Administrator**, **Manager**, **Operator**, **Guest**.

1. Select **Tools** > **Users and Roles**.
2. Select the ***Roles*** tab.
3. Select the check box(es) associated with the enabled custom role(s) you want to disable.
4. Click **Disable**.

**Result:** The selected role(s) is disabled.

**Caution:** If you disable a role currently assigned to a user, they can still log in to Lumension Endpoint Management and Security Suite, but their access rights are heavily restricted.

## Enabling User Roles

Re-enable disabled user roles to assign them to users. You can enable disabled user roles at any time.

Re-enable roles from the ***Roles*** tab.

1. Select **Tools** > **Users and Roles**.
2. Select the ***Roles*** tab.
3. Select the check box(es) associated with the disabled role(s) you want to enable.
4. Click **Enable**.

**Result:** The selected user role(s) is re-enabled. You can now assign it to users.

**Note:** Users already assigned the previously disabled role will again be able to access Lumension Endpoint Management and Security Suite with their full access rights.

## Deleting User Roles

Delete custom user roles when they are no longer needed. You can delete roles regardless of whether they are enabled or disabled. You cannot delete predefined system roles.

Delete roles from the ***Roles*** tab.

1. Select **Tools** > **Users and Roles**.
2. Select the ***Roles*** tab.
3. Delete the desired roles.

   Use one of the following methods.

| Method | Steps |
|---|---|
| **To delete a single user role:** | 1. Click the **Delete** icon associated with the role you want to delete.<br>2. Click **OK** to acknowledge the deletion. |
| **To delete multiple user roles:** | 1. Select the check boxes associated with the user roles that you want to delete.<br>2. From the toolbar, click the **Delete** button.<br>3. Click **OK** to acknowledge the deletion. |

**Note:** You cannot delete system roles: **Administrator**, **Manager**, **Operator**, **Guest**.

**Result:** The role is deleted.

**Caution:** If you delete a role currently assigned to a user, they can still log in to Lumension Endpoint Management and Security Suite, but their access rights are heavily restricted.

## Exporting User Role Data

You can export the data displayed on the ***Roles*** tab list so that it can be used in other applications. This data is exported to a comma separated value (`.csv`) file.

To export data, click the **Export** button. For additional information refer to *Exporting Data* on page 37.

# Chapter 12

# Using Lumension Installation Manager

**In this chapter:**


- Lumension Installation Manager
- Accessing Lumension Installation Manager
- The Navigation Menu
- The Home Page
- The New/Update Components Tab
- Working with Installs and Updates
- The Existing Components Tab
- Working with Uninstalls
- The Installation Log
- The Installation Manager Technical Support Page
- The Installation Manager Product Licensing Page


Lumension Installation Manager (Installation Manager) is a utility you can use to install, uninstall, or update Lumension Endpoint Management and Security Suite (Lumension EMSS) components.

Installation Manager is accessible following Lumension EMSS installation. Installation Manager provides flexibility; you can install, update, or uninstall components quickly and easily.

## Lumension Installation Manager

Lumension Endpoint Management and Security Suite (Lumension EMSS) is a platform that supports various solutions to security threats. These solutions are called modules. You can install new modules to the Lumension EMSS platform with the Lumension Installation Manager (Installation Manager). You can also use Installation Manager to upgrade modules or the Lumension EMSS platform itself.

Installation Manager is installed during the initial Lumension EMSS installation, and can be accessed following setup from the Lumension EMSS Web console. Use Installation Manager to install, update, or uninstall Lumension EMSS components: both platform components and module components. For additional information about these components, refer to *The Lumension Endpoint Management and Security Suite Components* on page 20.

Installation Manager allows for flexibility among module components. Each module is installed independently within the Lumension EMSS Web console. Based on which modules you have installed, different security solution features are available within the console.

**Notice:** Although most modules are not considered part of the Lumension EMSS platform, there are exceptions. The Wake on LAN module and the Lumension Remote Systems Management module are both installed with Lumension EMSS platform and cannot be uninstalled. Therefore, these modules are listed as platform components within Installation Manager.

## Accessing Lumension Installation Manager

Open Lumension Installation Manager to manage Lumension Endpoint Management and Security Suite components.

Lumension Installation Manager can be accessed using one of the following methods.

Table 111: Access Methods

| Access Method | Description |
|---|---|
| Lumension Endpoint Management and Security Suite | You can access the Lumension Installation Manager via the Lumension Endpoint Management and Security Suite Web console. Open the Web console, and then select the applicable menu item or click the applicable toolbar button to open the utility. For additional information, refer to *Accessing Installation Manager Via Lumension Endpoint Management and Security Suite* on page 276. |
| Windows Start Menu | You can also access the Lumension Installation Manager via the Windows Start Menu on the server that hosts Lumension Endpoint Management and Security Suite. For additional information, refer to *Accessing Installation Manager Via Windows* on page 277. |

**Note:** Only users assigned the *Administrator* role (or the *Manage Modules* access right) within Lumension Endpoint Management and Security Suite can access Installation Manager. Additionally, when accessing a Lumension Endpoint Management and Security Suite Server that uses SSL, Microsoft Silverlight may create notification dialogs that you must acknowledge.

### Accessing Installation Manager Via Lumension Endpoint Management and Security Suite

You can open Installation Manager using one of several pages within the Lumension Endpoint Management and Security Suite Web console.

You can perform this task from any endpoint in your network.

**Note:** Only users assigned the *Administrator* role or the **Installation Manager** access right within Lumension Endpoint Management and Security Suite can access Installation Manager.

1. Complete *Logging In to Lumension Endpoint Management and Security Suite* on page 27.

2. Open the Installation Manager in a new browser window using one of the following methods:

| Method | Steps |
|---|---|
| **Using the Navigation Menu:** | Select **Tools** > **Launch Installation Manager...**. |
| **Using the *Subscription Updates* page:** | 1. Select **Tools** > **Subscription Updates**.<br>2. From the toolbar, select **Launch Installation Manager...**. |
| **Using the *Product Licensing* page:** | 1. Select **Help** > **Subscription Updates**.<br>2. From the toolbar, select **Launch Installation Manager...**. |
| **Using the *System Alert* pane:** | 1. Click the system alert link.<br>**Note:** Only system alerts related to Installation Manager contain a link to open Installation Manager. |

**Result:** The Installation Manager opens in a new browser window to the ***New/Update Components*** tab.

**Note:** When accessing a Lumension Endpoint Management and Security Suite Server that uses SSL, Microsoft Silverlight may create notification dialogs that you must acknowledge.

## Accessing Installation Manager Via Windows

You can access Installation Manager using the Windows Start Menu.

Perform this task from the server that hosts Lumension Endpoint Management and Security Suite.

**Note:** Only users assigned the *Administrator* role or the **Installation Manager** access right within Lumension Endpoint Management and Security Suite can access Installation Manager.

Select **Start** > **All Programs** > **Lumension** > **Lumension Installation Manager**.

**Result:** Installation Manager opens in a new browser window to the ***New/Update Components*** tab.

**Note:** When accessing a Lumension Endpoint Management and Security Suite Server that uses SSL, Microsoft Silverlight may create notification dialogs that you must acknowledge.

## Logging Out

After you finish using Installation Manager, log out to ensure no unauthorized use takes place.

Log out of the Installation Manager browser window.

1. Click **Close**.

   **Step Result:** A confirmation dialog opens.

2. Click **Yes** to confirm closing the Installation Manager browser window.

**Result:** You are logged out of Installation Manager.

## The Navigation Menu

This menu appears on all Lumension Installation Manager pages. Use this menu to navigate through the Web console.

This menu organizes product features based on functionality. When you select a menu item, a new page or dialog opens. You can access all features of the system from this menu.

Table 112: Navigation Menu

| Menu | Menu Item | Function |
|---|---|---|
| **Home** | | Opens the entrance page to Lumension Installation Manager. For additional information, refer to *The Home Page* on page 279. |
| **Tools** | **View Install Log...** | Opens the ***Install Log*** dialog. For additional information, refer to *The Installation Log* on page 289 (dialog). |
| **Help** | **Help Topics...** | Opens the Lumension Endpoint Management and Security Suite Help system. For additional information, refer to *Help* on page 37. |
| | **Knowledge Base...** | Opens the Lumension Knowledge Base at *Lumension Support* (*http://support.lumension.com*). |
| | **Technical Support** | Opens the ***Technical Support*** page. For additional information, refer to *The Installation Manager Technical Support Page* on page 291. |
| | **Product Licensing** | Opens the ***Product Licensing*** page. For additional information, refer to *The Installation Manager Product Licensing Page* on page 294. |
| | **About...** | Opens the ***About*** dialog. |

# The Home Page

This page is the entrance page to Lumension Installation Manager.

This page contains the following tabs:

- *The New/Update Components Tab* on page 280
- *The Existing Components Tab* on page 286

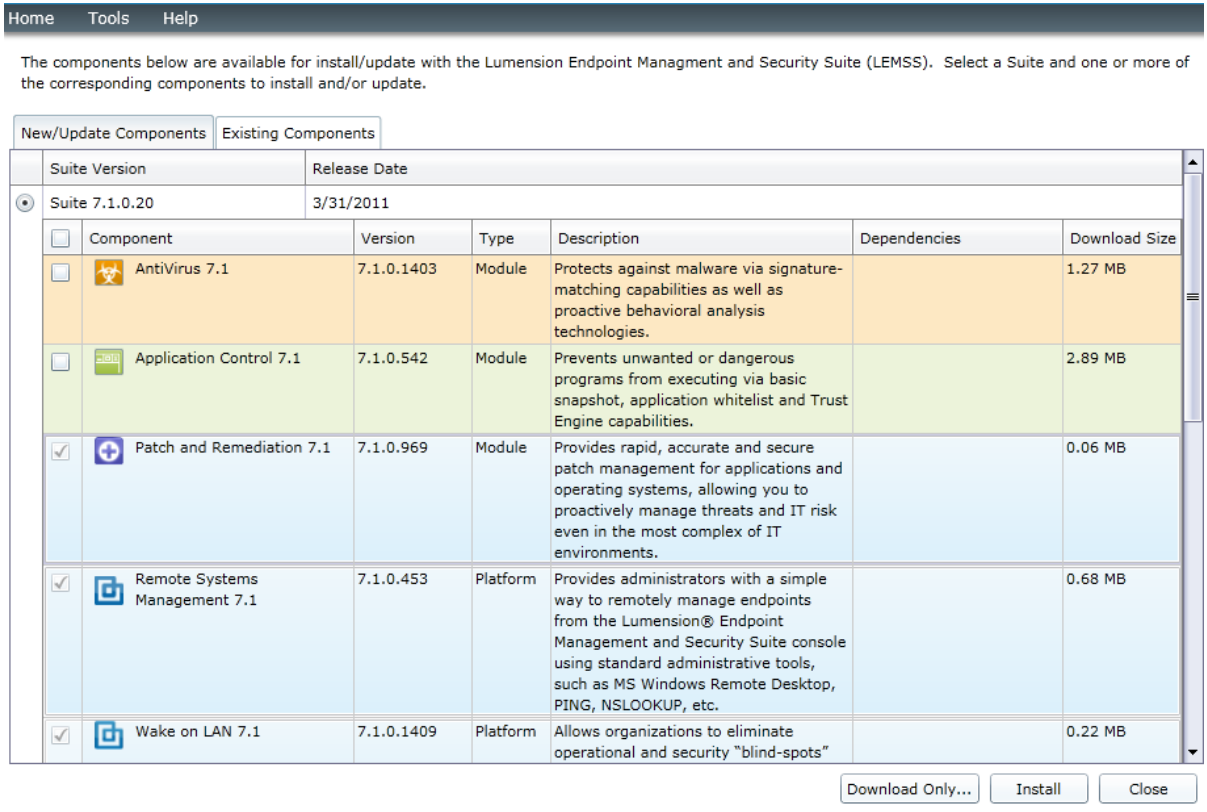

Home
Tools
Help
The components below are available for install/update with the Lumension Endpoint Managment and Security Suite (LEMSS). Select a Suite and one or more of the corresponding components to install and/or update.
New/Update Components
Existing Components
Suite Version
Release Date
Suite 7.1.0.20
3/31/2011
Component
Version
Type
Description
Dependencies
Download Size
AntiVirus 7.1
7.1.0.1403
Module
Protects against malware via signature-matching capabilities as well as proactive behavioral analysis technologies.
1.27 MB
Application Control 7.1
7.1.0.542
Module
Prevents unwanted or dangerous programs from executing via basic snapshot, application whitelist and Trust Engine capabilities.
2.89 MB
Patch and Remediation 7.1
7.1.0.969
Module
Provides rapid, accurate and secure patch management for applications and operating systems, allowing you to proactively manage threats and IT risk even in the most complex of IT environments.
0.06 MB
Remote Systems Management 7.1
7.1.0.453
Platform
Provides administrators with a simple way to remotely manage endpoints from the Lumension® Endpoint Management and Security Suite console using standard administrative tools, such as MS Windows Remote Desktop, PING, NSLOOKUP, etc.
0.68 MB
Wake on LAN 7.1
7.1.0.1409
Platform
Allows organizations to eliminate operational and security "blind-spots"
0.22 MB
Download Only...
Install
Close

Figure 104: Home Page

The tab that opens varies according to the method used to access Lumension Installation Manager.

# The New/Update Components Tab

Use this tab to manage components and your Lumension Endpoint Management and Security Suite version. This tab lists each yet-to-be installed component available for each Lumension Endpoint Management and Security Suite release.

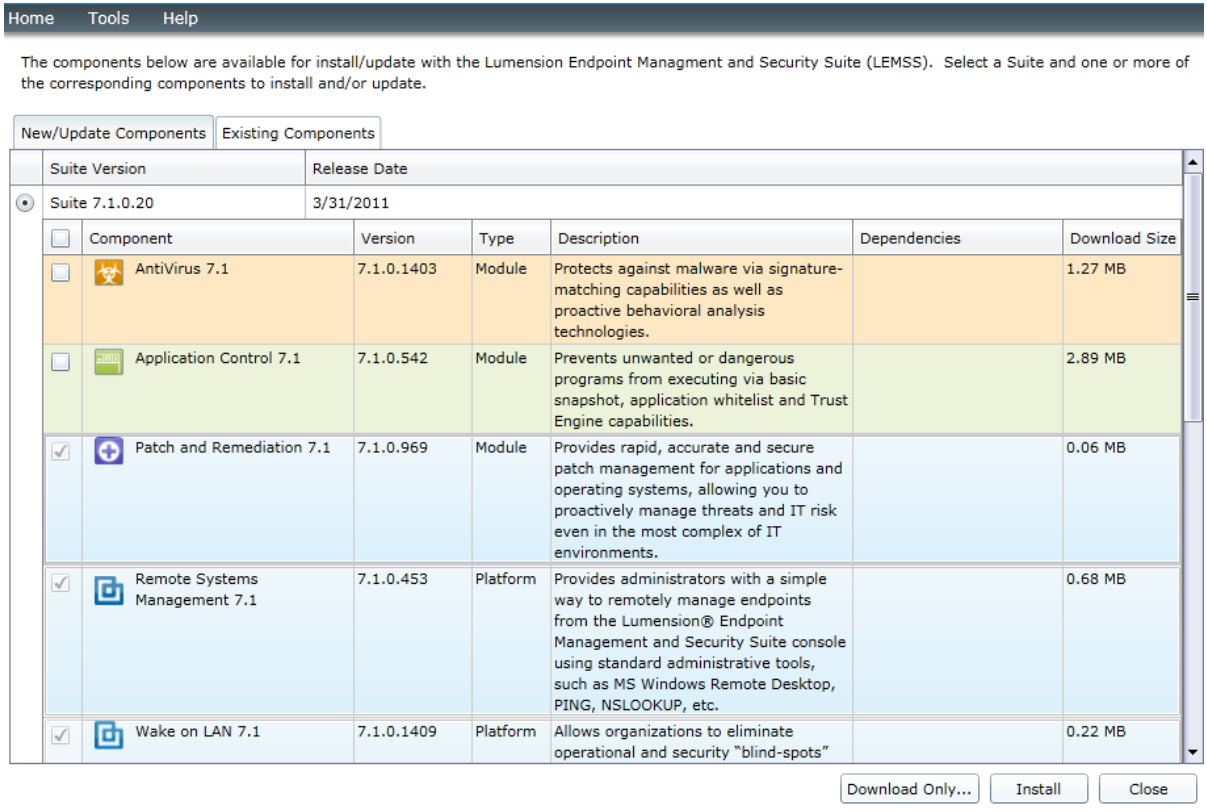

Home
Tools
Help
The components below are available for install/update with the Lumension Endpoint Managment and Security Suite (LEMSS). Select a Suite and one or more of the corresponding components to install and/or update.
New/Update Components
Existing Components
Suite Version
Release Date
Suite 7.1.0.20
3/31/2011
Component
Version
Type
Description
Dependencies
Download Size
AntiVirus 7.1
7.1.0.1403
Module
Protects against malware via signature-matching capabilities as well as proactive behavioral analysis technologies.
1.27 MB
Application Control 7.1
7.1.0.542
Module
Prevents unwanted or dangerous programs from executing via basic snapshot, application whitelist and Trust Engine capabilities.
2.89 MB
Patch and Remediation 7.1
7.1.0.969
Module
Provides rapid, accurate and secure patch management for applications and operating systems, allowing you to proactively manage threats and IT risk even in the most complex of IT environments.
0.06 MB
Remote Systems Management 7.1
7.1.0.453
Platform
Provides administrators with a simple way to remotely manage endpoints from the Lumension® Endpoint Management and Security Suite console using standard administrative tools, such as MS Windows Remote Desktop, PING, NSLOOKUP, etc.
0.68 MB
Wake on LAN 7.1
7.1.0.1409
Platform
Allows organizations to eliminate operational and security "blind-spots"
0.22 MB
Download Only...
Install
Close

Figure 105: New/Update Components Tab

Use this tab to complete the following component management tasks:

- Download components. For additional information, refer to *Downloading Components* on page 282.
- Install downloaded components. For additional information, refer to *Installing Downloaded Components* on page 283.
- Download and install components. For additional information, refer to *Installing or Updating Components* on page 284.
- Update components. For additional information, refer to *Installing Downloaded Components* on page 283.

When installing or upgrading, you can either install or download the applicable components.

## The New/Update Components Tab List

The tab list itemizes all unapplied components for each Lumension Endpoint Management and Security Suite (Lumension EMSS) release.

This list is separated into two tiers.

- Tier one lists the Lumension EMSS release.
- Tier two lists unapplied components for the applicable Lumension EMSS release.

The following table describes the first tier of the ***New/Update Components*** tab list.

Table 113: New/Update Components Tab List (Tier One)

| Column | Description |
|---|---|
| **Suite Version** | The version number of the applicable Lumension EMSS release. |
| **Release Date** | The date and time the associated Lumension EMSS update was released. |

The following table describes the second tier of the ***New/Update Components*** tab list. This tier lists the components available for the applicable Lumension EMSS release.

Table 114: New/Update Components Tab List (Tier Two)

| Column | Description |
|---|---|
| **Component** | The component available for installation. |
| **Version** | The version of the component. |
| **Type** | The type of component (`Platform` or `Module`). |
| **Description** | The description for the component. |
| **Dependencies** | The prerequisite component needed to install the component. |
| **Download Size** | The size of the component (in MBs). |

## The New/Update Components Tab Buttons

After selecting components from the ***New/Update Components*** tab list, use the available buttons to initiate installations or downloads.

The following table describes the ***New/Update Components*** tab button functions.

Table 115: New/Update Components Tab Buttons

| Button | Function |
|---|---|
| **Download Only...** | Downloads the selected components. For additional information, refer to *Downloading Components* on page 282. |
| **Install** | Installs the selected components. For additional information, refer to *Installing or Updating Components* on page 284. |

| Button | Function |
|---|---|
| **Close** | Closes Installation Manager. For additional information, refer to *Logging Out* on page 277 |

# Working with Installs and Updates

You can download, install, or update Lumension Endpoint Management and Security Suite components from the ***New/Update Components*** tab.

You can perform the following tasks from this tab:

- *Downloading Components* on page 282
- *Installing Downloaded Components* on page 283
- *Installing or Updating Components* on page 284

## Downloading Components

You can use the Lumension Installation Manager to download components for later installation.

Complete downloads from the ***New/Update Components*** tab within the Installation Manager Web console.

1. From the navigation menu, select **Home**.
2. Ensure the ***New/Update Components*** tab is selected.
3. Select the radio button associated with the Lumension Endpoint Management and Security Suite release you want to download content for.
4. Select the check box(es) associated with the component(s) you want to download.
5. Click **Download Only...**.

   **Step Result:** The ***Download Components*** dialog opens.

   **Note:** If downloading a component with unmet prerequisites, a notification dialog opens, prompting you to download the prerequisites. Click **Yes** to download the prerequisites or **No** to skip them. You cannot install the selected component(s) until the prerequisites are downloaded and installed.

6. Click **Close** when the download completes.

**Result:** The component is downloaded to the defined location or the default location (`<Installation Directory>\Lumension\EMSS\Content`).

**After Completing This Task:**

You may install the component at any time after downloading. Refer to *Installing Downloaded Components* on page 283 for install information.

## Installing Downloaded Components

You can use Lumension Installation Manager to install downloaded components.

**Prerequisites:**

The components require downloading. Refer to *Downloading Components* on page 282 for download information.

Complete install of downloaded components from the ***New/Update Components*** tab within the Installation Manager Web console.

1. From the navigation menu, select **Home**.
2. Ensure the ***New/Update Components*** tab is selected.
3. Select the radio button associated with Lumension Endpoint Management and Security Suite release for which you want to install content.
4. Select the check box(es) associated with the downloaded component(s) you want to install for.
5. Click **Install**.

   **Step Result:** The ***Install/Update Components*** dialog opens.

   **Note:** If installing component(s) that do not support module(s) currently installed, a notification dialog opens, prompting you to remove the module(s). Click **OK** to uninstall the applicable module(s). Failure to uninstall the applicable modules cancels the install. If installing a component with unmet prerequisites, a notification dialog opens, prompting you to install the prerequisites. Click **Yes** to install the prerequisites. Failure to install the prerequisites cancels the install.

6. Complete the applicable steps according the dialog page that opens.

   The following table describes the steps for each dialog page.

| Page | Step(s) |
|---|---|
| If the ***Prerequisites*** page opens: | Your server does not meet the recommended system requirements to install the selected content.<br>• If you receive *failure(s)*, you must cancel the installation and resolve the failures before you can install the content.<br>• If you receive *warning(s)*, you may proceed by clicking **Next**. Lumension recommends resolving the warning(s) before proceeding.<br>**Tip:** Click **Print** for a hard copy of prerequisite deficiencies. Click **Retry** to reassess the server. |

| Page | Step(s) |
| --- | --- |
| If the ***Ready to Install*** page opens: | 1. Review the content selected for installation.<br>2. Click **Install**.<br>**Tip:** Click the **terms and conditions link** to view the company terms and conditions. |

**Step Result:** The selected component(s) begin installing.

7. After installation completes, review the installation information.

**Tip:** If desired, click the **View install log** link to view the install log. For additional information, refer to *The Installation Log* on page 289.

8. If desired, select the check box to launch Lumension Endpoint Management and Security Suite after clicking **Finish**.
9. Click **Finish**.

**Result:** The downloaded component(s) are installed.

**After Completing This Task:**

Before you can begin using a newly installed module component, you must first install the module's endpoint component on endpoints hosting the Lumension EMSS Agent. For additional information, refer to *Enabling Modules on Endpoint* on page 168.

## Installing or Updating Components

You can use Lumension Installation Manager to download new or update existing components and install them automatically.

Complete installs from the ***New/Update Components*** tab within the Installation Manager Web console.

1. From the navigation menu, select **Home**.
2. Ensure the ***New/Update Components*** tab is selected.
3. Select the radio button associated with Lumension Endpoint Management and Security Suite release for which you want to install content.
4. Select the check box(es) associated with the component(s) you want to install or update.
5. Click **Install**.

**Step Result:** The ***Install/Update Components*** dialog opens.

**Note:** If installing component(s) that do not support module(s) currently installed, a notification dialog opens, prompting you to remove the module(s). Click **OK** to uninstall the applicable module(s). Failure to uninstall the applicable modules cancels the install. If installing a component with unmet prerequisites, a notification dialog opens, prompting you to install the prerequisites. Click **Yes** to install the prerequisites. Failure to install the prerequisites cancels the install.

6. Complete the applicable steps according the dialog page that opens.

   The following table describes the steps for each dialog page.

| Page | Step(s) |
|---|---|
| If the ***Prerequisites*** page opens: | Your server does not meet the recommended system requirements to install the selected content.<br>• If you receive *failure(s)*, you must cancel the installation and resolve the failures before you can install the content.<br>• If you receive *warning(s)*, you may proceed by clicking **Next**. Lumension recommends resolving the warning(s) before proceeding.<br>**Tip:** Click **Print** for a hard copy of prerequisite deficiencies. Click **Retry** to reassess the server. |
| If the ***Ready to Install*** page opens: | 1. Review the content selected for installation.<br>2. Click **Install**.<br>**Tip:** Click the **terms and conditions link** to view the company terms and conditions. |

   **Step Result:** The selected component(s) begin downloading and installing.

7. After installation completes, review the installation information.

   **Tip:** If desired, click the **View install log** link to view the install log. For additional information, refer to *The Installation Log* on page 289.

8. If desired, select the check box to launch Lumension Endpoint Management and Security Suite after clicking **Finish**.
9. Click **Finish**.

**Result:** The new component(s) are installed.

**After Completing This Task:**

Before you can begin using a newly installed module component, you must first install the module's endpoint component on endpoints hosting the Lumension EMSS Agent. For additional information, refer to *Managing Module Endpoint Components*.

# The Existing Components Tab

This tab lists the version of Lumension Endpoint Management and Security Suite currently installed on your server and the installed components.

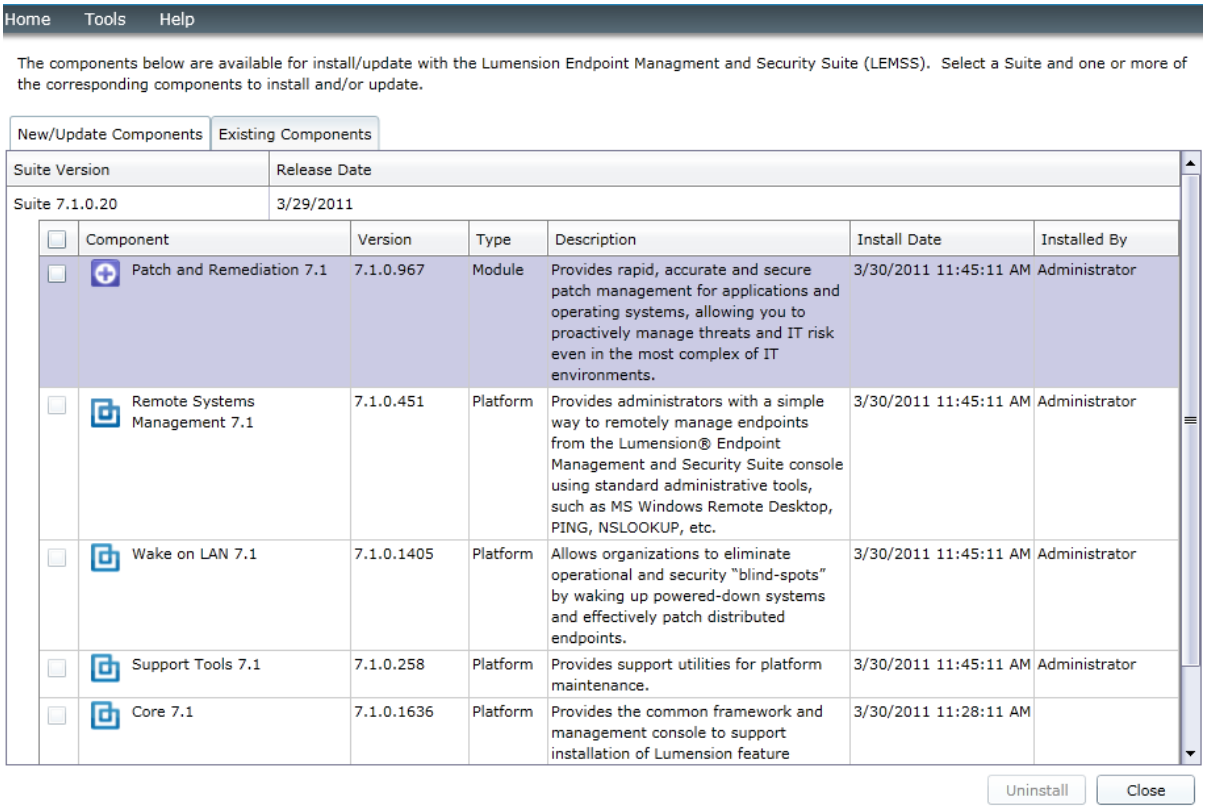

Home
Tools
Help
The components below are available for install/update with the Lumension Endpoint Managment and Security Suite (LEMSS). Select a Suite and one or more of the corresponding components to install and/or update.
New/Update Components
Existing Components
Suite Version
Release Date
Suite 7.1.0.20
3/29/2011
Component
Version
Type
Description
Install Date
Installed By
Patch and Remediation 7.1
7.1.0.967
Module
Provides rapid, accurate and secure patch management for applications and operating systems, allowing you to proactively manage threats and IT risk even in the most complex of IT environments.
3/30/2011 11:45:11 AM
Administrator
Remote Systems Management 7.1
7.1.0.451
Platform
Provides administrators with a simple way to remotely manage endpoints from the Lumension® Endpoint Management and Security Suite console using standard administrative tools, such as MS Windows Remote Desktop, PING, NSLOOKUP, etc.
3/30/2011 11:45:11 AM
Administrator
Wake on LAN 7.1
7.1.0.1405
Platform
Allows organizations to eliminate operational and security "blind-spots" by waking up powered-down systems and effectively patch distributed endpoints.
3/30/2011 11:45:11 AM
Administrator
Support Tools 7.1
7.1.0.258
Platform
Provides support utilities for platform maintenance.
3/30/2011 11:45:11 AM
Administrator
Core 7.1
7.1.0.1636
Platform
Provides the common framework and management console to support installation of Lumension feature
3/30/2011 11:28:11 AM
Uninstall
Close

Figure 106: Existing Components Tab

Use this tab to uninstall existing module components.

## The Existing Components Tab List

This list identifies which version of Lumension Endpoint Management and Security Suite (Lumension EMSS) is installed on your server and itemizes the components installed.

This list is separated into two tiers.

- Tier one lists the version of Lumension EMSS installed on your server.
- Tier two lists components installed on your platform. The list contains information about each platform and module component installed.

The following table describes the first tier of the ***Existing Components*** tab list.

Table 116: Existing Components Tab List (Tier One)

| Column | Description |
|---|---|
| **Suite Version** | The version number of the applicable Lumension EMSS release. |
| **Release Date** | The date and time the associated Lumension EMSS update was released. |

The following table describes the second tier of the ***Existing Components*** tab list.

Table 117: Existing Components Tab List (Tier Two)

| Column | Description |
|---|---|
| **Component** | The name of the component installed on your Lumension EMSS Server. |
| **Version** | The version of the component. |
| **Type** | The type of component (`Platform` or `Module`). |
| **Description** | The description for the component. |
| **Install Date** | The date and time the component was downloaded from the Global Subscription Server. |
| **Installed By** | The person who installed the component. |

### The Existing Components Tab Buttons

Use tab buttons to uninstall existing Lumension Endpoint Management and Security Suite module components.

The following table describes the ***Existing Components*** tab button functions.

| Button | Function |
|---|---|
| **Uninstall** | Uninstalls selected module components. For additional information, refer to *Uninstalling Module Components* on page 288.<br>**Note:** Platform components cannot be uninstalled. |
| **Close** | Closes the Lumension Installation Manager. |

## Working with Uninstalls

You can uninstall existing Lumension Endpoint Management and Security Suite module components from the ***Existing Components*** tab.

You can perform the following tasks from this tab:

- *Uninstalling Module Components* on page 288

## Uninstalling Module Components

You can uninstall module components when they are no longer used or needed.

Uninstall module components from the ***Existing Components*** tab within the Installation Manager Web console.

1. From the navigation menu, select **Home**.
2. Select the ***Existing Components*** tab.
3. From the list, select the module component(s) you want to uninstall.

   **Note:** You may have to uninstall dependent modules as well. Platform components cannot be uninstalled.

4. Click **Uninstall**.

   **Step Result:** The ***Uninstall Components*** dialog opens, listing the component you have selected to uninstall.

5. Click **Uninstall**.

   **Step Result:** A dialog opens, notifying you that all data associated with the selected components will be lost.

6. Click **Yes**.

   **Step Result:** The selected components begin uninstalling.

7. When the component removal finishes, a confirmation dialog listing uninstalled components displays.

   **Note:** If desired, select the one of the following:

   - Select the check box to launch Lumension Endpoint Management and Security Suite (Lumension EMSS) opens in a new browser window after you close the ***Uninstall Components*** dialog.
   - Click the **View install log** link to view the install log. For additional information, refer to *The Installation Log* on page 289.

8. Click **Finish**.

   **Step Result:** Closes the ***Uninstall Components*** dialog.

**Result:** The selected Lumension EMSS module component(s) are uninstalled.

# The Installation Log

The ***Installation Log*** is a dialog that lists details about Lumension Installation Manager events. The log lists occurrences from the last installation or removal of a component.

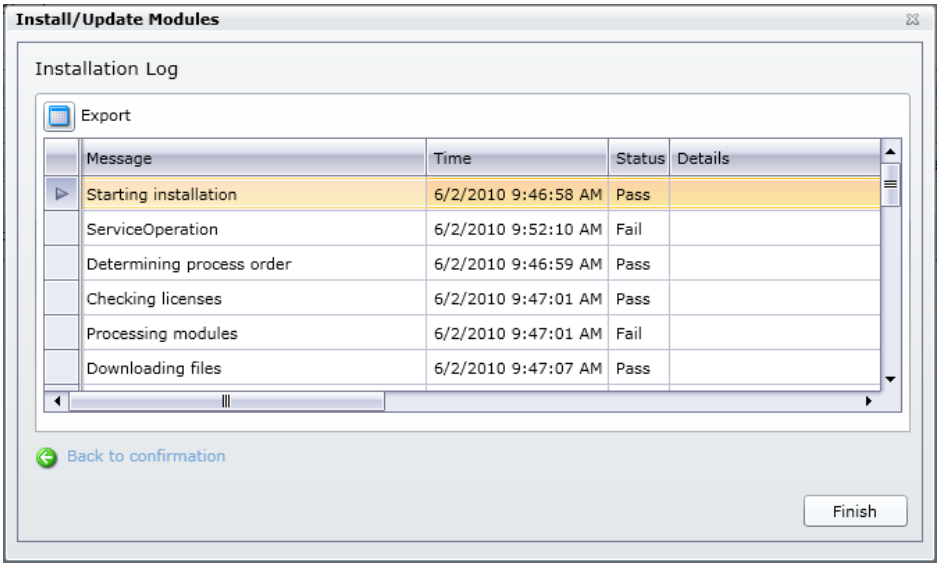



Figure 107: Installation Log

This log is especially useful for troubleshooting installation or removal failures. The log features a list and buttons.

## Viewing the Installation Log

View the ***Installation Log*** for details about the events that occurred during the most recent installation or removal of Lumension Endpoint Management and Security Suite components.

View the ***Installation Log*** using the navigation menu within the Installation Manager Web console.

**Tip:** You can view the ***Installation Log*** from various locations in the Lumension Installation Manager console. For additional information, refer to one of the following topics:

- *Installing or Updating Components* on page 284
- *Uninstalling Module Components* on page 288

1. Select **Tools** > **View Install Log...**.

   **Step Result:** The ***Installation Log*** opens.

2. Review the log details. For additional information, refer to *The Installation Log List* on page 290.

## The Installation Log List

After selected components are installed or removed, you may view a log of events that occurred during the process.

The following reference describes each column in installation log table.

Table 118: Installation Log Table Columns

| Column | Description |
|---|---|
| **Message** | The name of the event. |
| **Time** | The date and time the event occurred. |
| **Status** | The outcome of the event (`Pass` or `Fail`). |
| **Details** | The notes regarding the event. |

## The Installation Log Buttons

Use ***Installation Log*** buttons to perform tasks within the dialog.

The following table describes the ***Installation Log*** button functions.

Table 119: Install Log Buttons

| Button | Description |
|---|---|
| **Export** | Exports the ***Installation Log*** list data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37. |
| **Close** | Closes the ***Installation Log***. |

**Note:** When viewing the log following an installation completion or failure, a **back to confirmation** link is available. Click this link to return to the installer ***Confirmation*** page. This link is not available when opening the log via the navigation menu.

# The Installation Manager Technical Support Page

Use this page to contact technical support. Technical support provides assistance for Lumension Installation Manager or any other Lumension product.

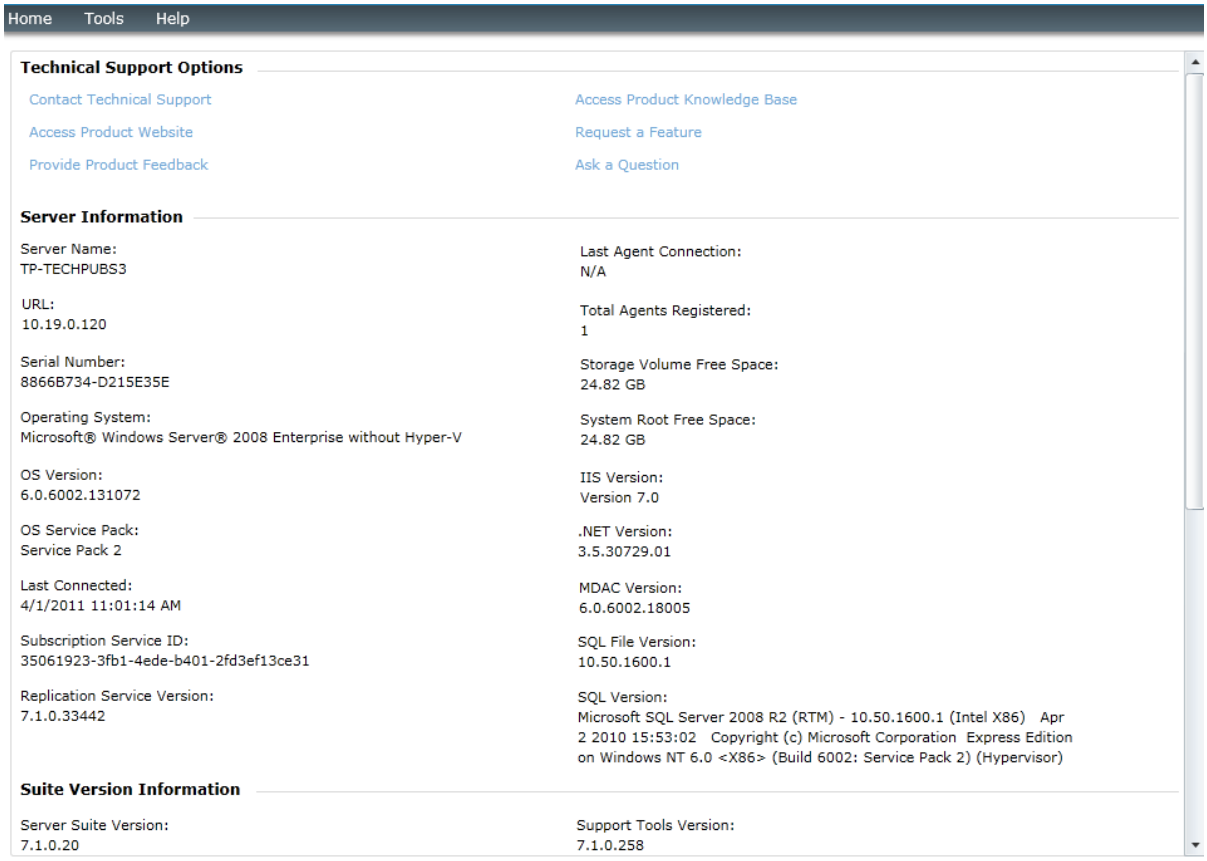



Figure 108: Technical Support Page

This page features multiple links to contact technical support. You can also use this page to provide comments for product improvement. This page also provides information about your Lumension Endpoint Management and Security Suite server and its components.

The page is divided into the following sections:

- *Technical Support Options* on page 292
- *Server Information* on page 292
- *The Installation Manager Technical Support Page* on page 291

## Viewing the Technical Support Page

Navigate to this page to access out-of-program technical support pages.

You can access this page at any time from the navigation menu.

1. Select **Help** > **Technical Support**.
2. View the page.

## Technical Support Options

Lumension Installation Manager provides access to various out-of-program technical support pages. Use these pages to communicate with Lumension. Click each link to open the applicable page in a new window.

The following table describes each link.

Table 120: Technical Support Options Links

| Link | Description |
|---|---|
| **Contact Technical Support** | Sends an email to technical support at *Lumension Support* (*patchlink.support@lumension.com*). |
| **Access Product Knowledge Base** | Accesses the knowledge base at *Lumension Support* (*http://support.lumension.com*). |
| **Access Product Web Site** | Accesses the *Lumension web site* (*http://www.lumension.com*). |
| **Request a Feature** | Sends a feature request to Lumension via the *Product Feedback and Feature Request Page* (*http://my.lumension.com/feedback.spring*). |
| **Provide Product Feedback** | Sends product input to Lumension via the *Product Feedback and Feature Request Page* (*http://my.lumension.com/feedback.spring*). |
| **Ask a Question** | Sends a support question to Lumension via the *Lumension Customer Portal* (*http://portal.lumension.com/*). |

## Server Information

These fields list general information regarding the Lumension Endpoint Management and Security Suite (Lumension EMSS) system.

Table 121: Server Information Fields

| Field | Description |
|---|---|
| **Server Name** | The name of the computer Lumension EMSS is installed on. |
| **Serial Number** | The serial number used by Lumension EMSS. |
| **Operating System** | The operating system installed and running on the Lumension EMSS Server. |
| **Last Connected** | The date and time Lumension EMSS last connected to the Global Subscription Server (GSS). |

| Field | Description |
|---|---|
| **Subscription Service ID** | The ID assigned to Lumension EMSS upon registration with the GSS. |
| **Replication Service Version** | The replication service version number. |
| **Operating System Version** | The operating system version number. |
| **URL** | The URL of the server Lumension EMSS is installed on. |
| **Last Agent Connection** | The date and time a registered Lumension EMSS Agent last connected to the Lumension EMSS Server. |
| **Storage Volume Free Space** | The amount of free disk space on your storage volume. |
| **System Root Free Space** | The amount of free disk space on your system volume. |
| **Total Agents Registered** | The total number of agents registered with Lumension EMSS. |

## Suite Version Information

**Suite Version Information** displays the version number of Lumension Endpoint Management and Security Suite (Lumension EMSS), each platform component installed, and each module component installed.

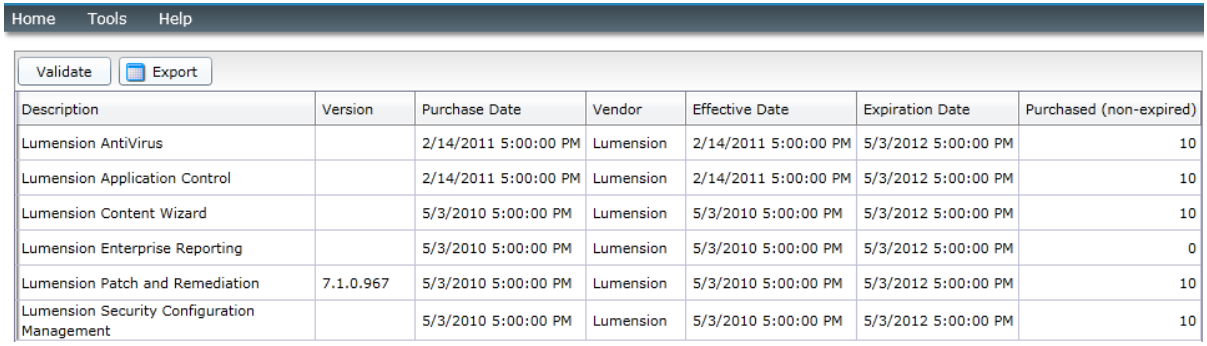
The following table describes each **Suite Version Information** field.

Table 122: Suite Version Information Fields

| Field | Description |
|---|---|
| **Server Suite Version** | The version number of Lumension EMSS installed on your Lumension EMSS server. |
| **Core Version** | The version number of the Lumension EMSS core installed on your Lumension EMSS server. |
| ***Module* Version** | The name and version number of a Lumension EMSS module installed on your Lumension EMSS server. A field appears for each module installed on your server. |

# The Installation Manager Product Licensing Page

Use this page to view, validate, and export license information. It summarizes product component licenses applicable to your endpoint management activities including their expiration date. Product information is updated during daily replication with the Global Subscription Server.




| Description | Version | Purchase Date | Vendor | Effective Date | Expiration Date | Purchased (non-expired) |
|---|---|---|---|---|---|---|
| Lumension AntiVirus | | 2/14/2011 5:00:00 PM | Lumension | 2/14/2011 5:00:00 PM | 5/3/2012 5:00:00 PM | 10 |
| Lumension Application Control | | 2/14/2011 5:00:00 PM | Lumension | 2/14/2011 5:00:00 PM | 5/3/2012 5:00:00 PM | 10 |
| Lumension Content Wizard | | 5/3/2010 5:00:00 PM | Lumension | 5/3/2010 5:00:00 PM | 5/3/2012 5:00:00 PM | 10 |
| Lumension Enterprise Reporting | | 5/3/2010 5:00:00 PM | Lumension | 5/3/2010 5:00:00 PM | 5/3/2012 5:00:00 PM | 0 |
| Lumension Patch and Remediation | 7.1.0.967 | 5/3/2010 5:00:00 PM | Lumension | 5/3/2010 5:00:00 PM | 5/3/2012 5:00:00 PM | 10 |
| Lumension Security Configuration Management | | 5/3/2010 5:00:00 PM | Lumension | 5/3/2010 5:00:00 PM | 5/3/2012 5:00:00 PM | 10 |

Figure 109: Product Licensing Page

## Viewing the Product Licensing Page

View this page for information about the modules you are currently licensed for.

View the ***Product Licensing*** page using the navigation bar.

Select **Tools** > **Product Licensing**.

**Result:** The ***Product Licensing*** page opens.

## The Product Licensing Page Buttons

Click these buttons to use functions related to licensing information.

The following table describes each button.

Table 123: Product Licensing Page Buttons

| Button | Function |
|---|---|
| **Validate** | Initiates a license replication that searches for any changes to your license data. For additional information, refer to *Validating License Information* on page 295. |
| **Export** | Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to *Exporting Data* on page 37.<br>**Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled. |

## The Product Licensing Page List

The page list itemizes information about each Lumension Endpoint Management and Security Suite module you are licensed for.

The following table describes each ***Product Licensing*** page list column.

Table 124: Product Licensing Page List Column

| Column | Description |
|---|---|
| **Description** | The module you are licensed for. |
| **Version** | The version number of the module. |
| **Purchase Date** | The date and time you purchased the module. |
| **Vendor** | The vendor that you purchased the module from. |
| **Effective Date** | The date that the module went into effect (not necessarily the purchase date). |
| **Expiration Date** | The date the module licensing expires. |
| **Purchased** | The total number of licences purchased for the module. |

## Validating License Information

Validating license information refreshes information about how many module licenses are available and in use. Validate license information after installing new modules.

Validate license information from the ***Product Licensing*** page.

1. Select **Help** > **Product Licensing**.
2. Click **Validate**.

# Chapter 13

# Using the Lumension Endpoint Management and Security Suite Agent

**In this chapter:**


- Upgrading Agents on Endpoints
- The Agent Control Panel
- The Summary Panel
- The Proxy Server Panel


The Lumension Endpoint Management and Security Suite (Lumension EMSS) Agent is the link between the host endpoint and its Lumension EMSS Server. The Lumension EMSS Agent scans the endpoint for inventory and uploads the scan results to the Lumension EMSS server. You can view these scan results from the Lumension EMSS Web console at any time, regardless of the scanned endpoint's network connectivity.

The agent also initiates system tasks deployed by the Lumension EMSS Server, such as endpoint reboots.

The agent also supports snap-ins for each Lumension EMSS module. By installing these agent modules, the agent's functionality can be expanded.

**Note:** Functions for each Lumension EMSS Agent module may only be accessible from separate user interfaces.

After installing the Lumension EMSS Agent, no additional user action is generally required. However, Lumension EMSS my be configured to require endpoint user interaction for activities such as endpoint reboots, deployments, and so on.

## Upgrading Agents on Endpoints

Upgrading an agent on an endpoint installs an updated version of the agent on the endpoint.

Versions of the Lumension Endpoint Management and Security Suite Agent 7.0 or later can be upgraded using the Lumension Endpoint Management and Security Suite Web console. During upgrades, the agent data and configuration is maintained. For additional information, refer to one of the following topics:

- To upgrade agents based on a complete list of endpoints in the system, refer to *Defining the Endpoint Agent Version* on page 166
- To upgrade agents based on individual endpoints*Defining the Endpoint Agent Version (Endpoint Details)* on page 181
- To upgrade agents based on groups, refer to *Defining the Endpoint Agent Version (Groups Page)* on page 205.

The 6.3 and 6.4 versions of the Lumension Endpoint Management and Security Suite Agents are not upgradeable. Rather, they must be overwritten. Overwrite 6.3 and 6.4 versions of the agent using one of the following methods:

- Use a third-party software distribution application to upgrade the agent.
- Download the appropriate installer to the endpoint that you want to manage, then run the installer locally on the endpoint. For more information, see *Downloading the Agent Installer* on page 166.
- Create an agent management job to install the agent that targets the endpoint (Windows operating systems only). When the job executes, an agent is installed on the endpoint. For more information, see *Installing Agents by Agent Management Job* on page 111.

# The Agent Control Panel

The ***Agent Control Panel*** is the interface used to control the Lumension Endpoint Management and Security Suite Agent. After installing the agent, you can view information about the agent and the modules it supports from this panel.

Use this control panel to manage Lumension Endpoint Management and Security Suite agent functionality. The control panel contains numerous several tabs. Based on the agent modules installed, different tab are displayed.

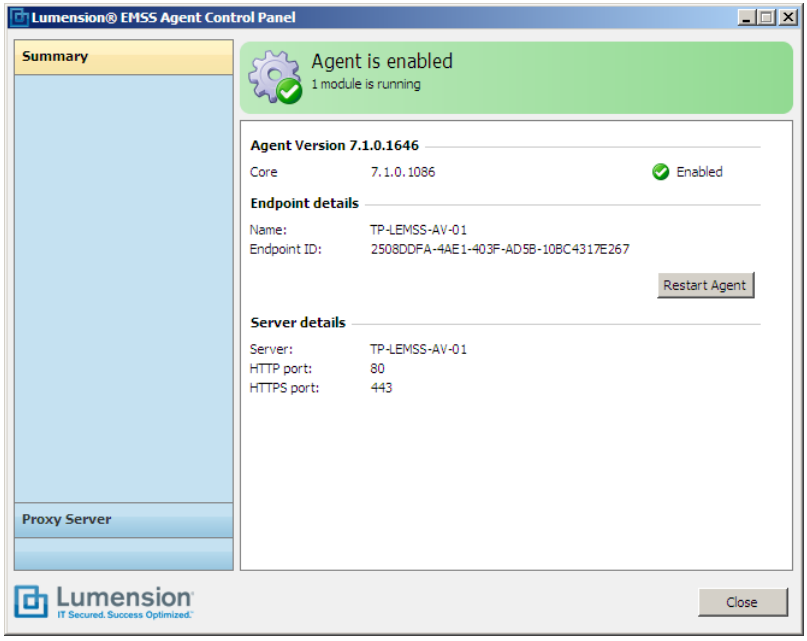



Figure 110: Agent Control Panel

The ***Agent Control Panel*** contains the following features:

| | |
|---|---|
| **Status Banner** | This banner indicates the current status of the agent. |
| **Main Menu** | This menu contains items for viewing general and module-specific information about the agent. Additional menu items appear each time a new module is installed. Select a menu item to display related information in the main panel.<br>This menu contains the following items:<br>• *The Summary Panel* on page 300<br>•<br>**Note:** Additional menu items are added and removed as modules are installed or uninstalled on the agent. |

| | |
|---|---|
| **Main Panel** | This panel displays information related to the selected menu item. |

### Accessing the Agent Control Panel

Access the panel to view and edit agent information.

Access the ***Agent Control Panel*** from an endpoint hosting a Lumension Endpoint Management and Security Suite Agent.

1. Select **Start** > **Control Panel**.
2. Double-click **Lumension EMSS Agent**.

**Result:** The ***Agent Control Panel*** opens to the ***Summary*** panel.

## The Summary Panel

This panel displays agent information, endpoint details, and server details. This panel is the ***Agent Control Panel*** default panel.

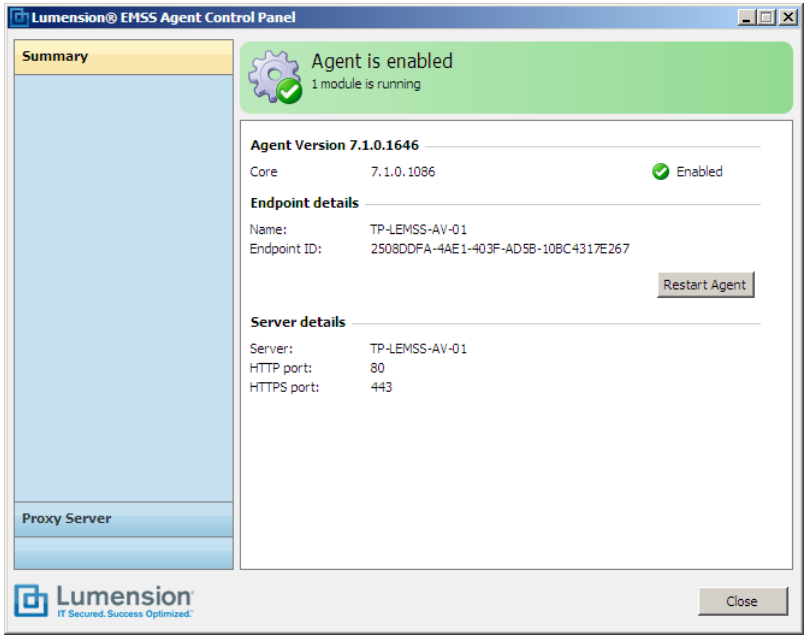



Figure 111: Summary Panel

This panel contains the following sections:

- *Agent Information* on page 301
- *Endpoint Details* on page 301
- *Server Details* on page 302

## Agent Information

This section lists the agent version and the module versions installed on the agent.

The following table defines each **Agent Information** field.

**Note:** Module entries only display when the applicable module is installed.

| Field | Description |
|---|---|
| Agent Version | Indicates the agent manifest in use. The manifest defines the agent modules available for installation. |
| Core | Indicates the version number of the Lumension Endpoint Management and Security Suite core installed. |

**Note:** For each field, an icon and accompanying text indicate the component status.

## Endpoint Details

This sections lists information about the endpoint hosting the agent.

The following table describes each **Endpoint details** field.

Table 125: Endpoint Detail Descriptions

| Field | Description |
|---|---|
| **Name** | The name of the endpoint hosting the agent. |
| **Endpoint ID** | The ID assigned to the endpoint by Lumension Endpoint Management and Security Suite. |

This section also features a **Restart Agent** button, which restarts the agent. For additional information, refer to *Restarting the Lumension Endpoint Management and Security Suite Agent* on page 301.

### Restarting the Lumension Endpoint Management and Security Suite Agent

If needed, you can restart the Lumension Endpoint Management and Security Suite Agent using the ***Agent Control Panel***.

Restart the agent from the ***Summary*** panel.

1. Select the ***Summary*** panel.
2. Click **Restart**.

**Result:** The agent is restarted.

### Server Details

This section lists information about the Lumension Endpoint Management and Security Suite (Lumension EMSS) Server the agent reports to.

The following table describes each **Server details** field.

Table 126: Server Details Field Descriptions

| Field | Description |
|---|---|
| **Server Identity** | The name of the Lumension EMSS Server in `http://ServerName.com` format.<br>**Note:** If a proxy server is configured, the proxy name displays in the **Server Identity** field. |
| **HTTP port** | The port number the server uses for communication with the agent. |
| **HTTPS port** | The port number the server uses for secure communication with the agent. |

## The Proxy Server Panel

This panel lists information related to proxy details for the endpoint.

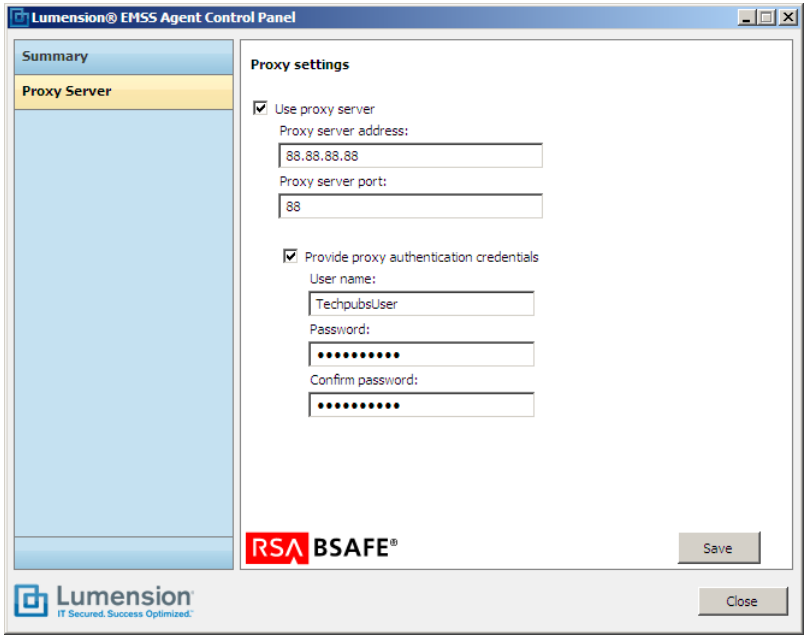



Figure 112: Proxy Server Panel

Proxy server settings are defined from the Proxy Server panel. To have your agent connect to the Lumension Endpoint Management and Security Suite server using a proxy server, define this panel.

## Defining Proxy Settings

If you access to disable server proxy settings, you may define your own proxy settings.

Edit proxy settings from the ***Proxy Server*** panel.

1. Select **Proxy Server** from the main menu.
2. Select the **Use proxy server** check box.
3. In **Proxy server address** field, type the proxy server IP address.
4. In the **Proxy server port** field, type the proxy server port used for communication between the agent and Lumension Endpoint Management and Security Suite server.
5. If the proxy server required authentication, complete the following substeps.
   a) Select the **Provide proxy authentication credentials** check box.
   b) In the **User Name** field, type a user name that authenticates with the proxy.
   c) In the **Password** field, type the password associated with the user name.
   d) In the **Re-enter password** field, re-type the password.
6. Click **Save**.

# Appendix
# A

# Server Reference

**In this appendix:**

- Server Security
- Server Error Pages
- WinInet Error Codes
- HTTP Status Codes
- Defining Targets Using Wildcards
- Defining Targets Within an Imported File
- Setting Up Lumension Endpoint Management and Security Suite
- Restarting the STATEngine Service

Within Lumension Endpoint Management and Security Suite, certain pages or code messages notify you of errors or events.

Refer to this appendix for a thorough definition of these pages and codes messages. This appendix also contains reference information regarding endpoint statuses, how to define scan targets using imported files, and how to restart the STATEngine Service.

## Server Security

Lumension Endpoint Management and Security Suite (Lumension EMSS) limits access to only authorized users. Referring to the definitions in this topic will help you understand how security operates within Windows and the product.

There are multiple layers of security for Lumension EMSS. These layers include:

| | |
|---|---|
| **Web Site Authentication** | Internet Information Services (IIS) controls authentication for access to the Lumension EMSS Web site, which means the operating system itself is validating credentials. |
| **Web Site Encryption via SSL** | SSL provides an encrypted wrapper around all Web communication to and from the product. Therefore, installing Lumension EMSS with SSL provides an additional level of protection. |

| | |
|---|---|
| **User (Security) Roles** | Every feature, page, and action throughout Lumension EMSS is assigned to a series of access rights. These access rights combine to form a user role. Roles also contain a list of accessible endpoints and endpoint groups. Regardless of how a user is authenticated, the access and permissions are defined solely by the Lumension EMSS administrator. |

## Server Error Pages

When an error occurs within Lumension Endpoint Management and Security Suite (Lumension EMSS), a special page opens that explains the error. Understanding these pages and what they mean will help you resume operations.

The Lumension EMSS server provides several distinct error pages. These pages are:

| | |
|---|---|
| **Access Denied** | Displays when a user fails to provide valid credentials during log in to the Lumension EMSS server. Also display when a user attempts to access a page or feature they do not have access to. |
| **Internal Server Error** | Displays when an unspecified internal error occurs. In most cases, closing the browser window and restarting your task will resolve the issue. |
| **Refresh User Data** | Displays when the current session expires. Usually displays following an extended period of inactivity. |
| **Requested Page Not Found** | Displays when a user attempts to navigate to a nonexistent server address. This page features links to other pages. Users can navigate from these links back to the desired page. |
| **System Component Version Conflict** | Displays when a system component version conflict is detected. To ensure optimal behavior, the system components of Lumension EMSS are checked every time a user logs in. If a conflict is detected, this page identifies the component(s) that caused the conflict.<br><br>**Note:** Lumension EMSS also sends a notification email to the Lumension EMSS administrator when a conflict occurs. |
| **Cache Expired** | Displays when the user session expires. Usually displays following an extended period of inactivity. |
| **Unsupported Browser Version** | Displays when a user attempts to open the Lumension EMSS server with an unsupported browser. |

## WinInet Error Codes

Lumension Endpoint Management and Security Suite uses Microsoft Window Internet application programming interface (WinInet API) for communication between the server and agents. When agent-server communication fails, a WinInet error code displays. Understanding these codes can help you resolve the communication errors.

The following table defines the most common error codes.

**Note:** Refer to *Microsoft Knowledgebase article #193625* (*http://support.microsoft.com/default.aspx?scid=kb;EN-US;193625*) for additional WinInet error code descriptions.

Table 127: WinInet Error Code Descriptions

| Agent Error Description | WinInet Error Code | Description |
|---|---|---|
| `Head failed: Head request failed. Error is 12002. . Host=1116 HTTP Error=0` | `12002` | The Internet connection timed out. |
| `Head failed: Head request failed. Error is 12031. . Host=1109 HTTP Error=0` | `12031` | The connection with the server has been reset. |
| `Head failed: Head request failed. Error is 12007. . Host=1109 HTTP Error=0` | `12007` | The server name could not be resolved. |

## HTTP Status Codes

As a Web-based application that uses Internet Information Services (IIS), Lumension Endpoint Management and Security Suite (Lumension EMSS) subsequently uses HTTP status codes. These codes appear when an HTTP error occurs while using the product. Understanding these codes will help you solve any issue that may arise.

While many of the status codes are informational only, the following table defines a few of the common error codes.

Table 128: HTTP Status Codes

| Code | Description |
|---|---|
| `HTTP 401.1 - Login failed` | Log in attempt was unsuccessful (typically due to invalid user name or password).<br>**Note:** Lumension EMSS will display a custom error page (as defined under *Server Error Pages* on page 306) instead of the default ***HTTP 401.1 - Logon failed*** error page. |
| `HTTP 403.4 - SSL required` | You must use HTTPS instead of HTTP when accessing this page. |

| Code | Description |
|---|---|
| `HTTP 403.9 - Too many users` | The number of connected users exceeds the defined connection limit. |
| `HTTP 404 - Not found` | The requested file cannot be found.<br>**Note:** Lumension EMSS will display a custom error page (as defined under *Server Error Pages* on page 306) instead of the default ***HTTP 404 - Not Found*** error page. |

## Defining Targets Using Wildcards

When configuring a discovery scan job or agent management job, you can define scan targets using *wildcard* IP addresses. Wildcards are characters can be used to substitute for any other character or characters in a string. In otherwords, you can use wildcards to scan for numerous IP address instead of just one. Use wildcards to scan specific IP address ranges.

The following table lists examples of how to define targets using wildcards.

Table 129: Wildcard Examples

| Discovery Method | Step | Example | Targets Defined |
|---|---|---|---|
| To define wildcard IP addresses: | Type a wildcard IP address using commas (,).<br>Type a wildcard IP address using dashes (-).<br>Type a wildcard IP address using asterisks (*).<br>Type a wildcard IP address using Classless Inter-Domain Routing (CIDR). | 10.1.1.2,9<br>10.1.1.2-5<br>10.1.1.*<br>10.1.1.0/24 | 10.1.1.2 and 10.1.1.9<br>10.1.1.2, 10.1.1.3, 10.1.1.4, and 10.1.1.5<br>10.1.1.0 through 10.1.1.255<br>10.1.1.0 through 10.1.1.255 |
| To define IP ranges: | Type two IP addresses separated by a greater-than sign (>).<br>Type two IP addresses separated by a dash (-).<br>**Note:** Dashes and greater-than signs are interchangeable. | 10.1.1.2 > 10.1.1.9<br>10.1.1.2 - 10.1.1.9 | 10.1.1.2 through 10.1.1.9<br>10.1.1.2 through 10.1.1.9 |

| Discovery Method | Step | Example | Targets Defined |
|---|---|---|---|
| To define wildcard IP addresses using dashes in various octets: | Type a wildcard IP address using dashes, placing the dashes where applicable. You can use dashes in any octet. | 10.2-4.5.9<br>10.5.2-4.9 | 10.2.5.9, 10.3.5.9, 10.4.5.9<br>10.5.2.9, 10.5.3.9, 10.5.4.9 |
| To define wildcard IP addresses using asterisks in various octets: | Type a wildcard IP address using asterisks, placing the asterisks where applicable. You can use asterisks in any octet. | *.6.65.92<br>10.25.*.* | 1.6.65.92 through 255.6.65.92<br>10.35.0.0 through 10.35.255.255 |
| To define wildcard IP addresses using commas in various octets: | Type a wildcard IP address using commas, placing the commas where applicable. You can use commas in any octet. | 10.2.5,9,12.9<br>10,12,19.2.5.9 | 10.2.5.9, 10.2.9.9, 10.2.12.9<br>10.2.5.9, 12.2.5.9, 19.2.5.9 |
| To define wildcard IP addresses using a combination of wildcard characters: | Type a wildcard IP address using dashes, commas, and asterisks. | 10-13.*.12.2,4,7<br>10.2-4.5,23.* | 10, 11, 12, 13.0-255.12.2, 4, 7<br>10.2, 3, 4.5, 23.0-255 |

## Defining Targets Within an Imported File

Using imported files, you can define job targets using a combination of single IP addresses, wildcard IP addresses, IP ranges, DNS names, NetBIOS names, and so on. To create a file containing targets, open a text

editor that allows you to create `.txt` or `.csv` (like Notepad). This topic also explains how to use wildcards for any job type.

The following table lists the methods you can use to define discovery methods within an importable file type, and then follows those methods with examples. Use one method per line.

Table 130: Basic Use

| Discovery Method | Step | Example | Targets Defined |
|---|---|---|---|
| To define single IP addresses: | Type a single address. | 10.1.1.2 | 10.1.1.2 |
| To define wildcard IP addresses: | Type a wildcard IP address using commas (,).<br>Type a wildcard IP address using dashes (-).<br>Type a wildcard IP address using asterisks (*).<br>Type a wildcard IP address using Classless Inter-Domain Routing (CIDR). | 10.1.1.2,9<br>10.1.1.2-5<br>10.1.1.*<br>10.1.1.0/24 | 10.1.1.2 and 10.1.1.9<br>10.1.1.2, 10.1.1.3, 10.1.1.4, and 10.1.1.5<br>10.1.1.0 through 10.1.1.255<br>10.1.1.0 through 10.1.1.255 |
| To define IP ranges: | Type two IP addresses separated by a greater-than sign (>).<br>Type two IP addresses separated by a dash (-).<br>**Note:** Dashes and greater-than signs are interchangeable. | 10.1.1.2 > 10.1.1.9<br>10.1.1.2 - 10.1.1.9 | 10.1.1.2 through 10.1.1.9<br>10.1.1.2 through 10.1.1.9 |
| To define DNS names: | Type a DNS host name for an endpoint. | DNS.dom.com | The defined DNS name. |

| Discovery Method | Step | Example | Targets Defined |
|---|---|---|---|
| To define NetBIOS names: | Type a NetBIOS name for an endpoint. | NetBIOSname | The defined NetBIOS name. |

Table 131: Advanced Use

| Discovery Method | Steps | Examples | Targets Defined |
|---|---|---|---|
| To define wildcard IP addresses using dashes in various octets: | Type a wildcard IP address using dashes, placing the dashes where applicable. You can use dashes in any octet. | 10.2-4.5.9<br>10.5.2-4.9 | 10.2.5.9, 10.3.5.9, 10.4.5.9<br>10.5.2.9, 10.5.3.9, 10.5.4.9 |
| To define wildcard IP addresses using asterisks in various octets: | Type a wildcard IP address using asterisks, placing the asterisks where applicable. You can use asterisks in any octet. | *.6.65.92<br>10.25.*.* | 1.6.65.92 through 255.6.65.92<br>10.35.0.0 through 10.35.255.255 |
| To define wildcard IP addresses using commas in various octets: | Type a wildcard IP address using commas, placing the commas where applicable. You can use commas in any octet. | 10.2.5,9,12.9<br>10,12,19.2.5.9 | 10.2.5.9, 10.2.9.9, 10.2.12.9<br>10.2.5.9, 12.2.5.9, 19.2.5.9 |
| To define wildcard IP addresses using a combination of wildcard characters: | Type a wildcard IP address using dashes, commas, and asterisks. | 10-13.*.12.2,4,7<br>10.2-4.5,23.* | 10, 11, 12, 13.0-255.12.2, 4, 7<br>10.2, 3, 4.5, 23.0-255 |

## Setting Up Lumension Endpoint Management and Security Suite

Following installation and initial log in, the ***Application Setup Manager*** dialog opens. This dialog appears only once, the first time you log in to Lumension Endpoint Management and Security Suite (Lumension EMSS) and you use it to configure basic options within the system.

**Prerequisites:**

Complete Lumension EMSS installation and open the Web console in your browser.

You cannot reopen this dialog following its completion. However, you can access these settings from various Lumension EMSS pages.

1. Log in to Lumension EMSS. For additional information, refer to *Logging In to Lumension Endpoint Management and Security Suite* on page 27.

   **Step Result:** Lumension EMSS opens and the ***Application Setup Manager*** displays. This dialog only appears the first time Lumension EMSS is opened.

2. Ensure the ***Customer Info*** tab is selected.
3. Type the applicable information in the following fields.

| Field | Description |
|---|---|
| **First name** | Your first name. |
| **Last name** | Your last name. |
| **Company name** | Your company name. The company name specified during installation appears by default but can be edited. |

4. Click **Apply**.
5. Click **Apply**.
6. Select the ***Uninstall Password**** tab.
7. Define the global agent uninstall password.
   This password can be used to manually uninstall Lumension EMSS agents and should be kept confidential.

**Tip:** For information on how to edit this password outside of the ***Application Setup Manager***, refer to *Defining the Global Uninstall Password* on page 229.

8. Click **Apply**.
9. Select the ***Email Notifications*** tab.
10. Define the email information used for email notifications.

    Email notifications are alerts sent by Lumension EMSS when certain system events occur.

    Type the applicable information in the following fields.

| Field | Description |
|---|---|
| **SMTP Host** | The local SMTP mail host name. Lumension EMSS uses your corporate Internet (SMTP) mail server. |
| **'From' email address** | The email address used when the system sends email notifications. |
| **'To' email address** | An email address you use to receive system notifications. |

**Important:** When upgrading Lumension EMSS via a fresh installation, you must reconfigure your email notifications after installing your licensed server modules. For additional details regarding Email Notifications, refer to The Email Notifications Page section within the *Lumension Endpoint Management and Security Suite 7.1 User Guide* (*http://portal.lumension.com*).

11. Click **Apply**.
12. Select the ***Install an Agent*** tab.
13. If desired, select the **Automatically install an agent on the server** check box to install an agent on the server.
    a) Select the check boxes the applicable modules.
       Selecting these modules activates agent functionality associated with the module.

> **Tip:** For additional information about installing an agent on the server outside of the ***Application Setup Manager***, refer to *Downloading the Agent Installer* on page 166.

14. Click **Apply**.

    **Step Result:** You initial settings are applied.

15. Click **Close**.

**Result:** Initial configuration is complete. You are now ready to begin monitoring your network with Lumension EMSS.

## Restarting the STATEngine Service

If the STATEngine service is disabled on the Lumension Endpoint Management and Security Suite, you will need to restart it before you can successfully complete discovery scan jobs and agent management jobs.

You can restart the STATEngine service from your server's command prompt.

> **Note:** If you try to configure a discovery scan job or agent management job while the STATEngine service is stopped, a dialog will open, notifying you that the engine is stopped.

1. Select **Start** > **Run**.
2. Type `net start statengine`.
3. Click **OK**.

**Result:** The STATEngine is restarted. You can now configure discovery scan jobs and agent management jobs.

# Appendix
# B

# Securing Your Server

**In this appendix:**


- Secure Your Server With SSL
- Use Secure Passwords
- Disabling File and Printer Sharing
- Placing Your Server Behind a Firewall
- Disable Non-Critical Services
- Lock Down Unused TCP and UDP Ports
- Apply All Security Patches


Lumension Endpoint Management and Security Suite protects your network endpoints. Server operation is critical to your network's overall security. To ensure your server is secure as possible, Lumension suggests implementing several security practices.

These practices include:

- Securing your server with SSL
- Using secure passwords
- Disabling file and printer sharing
- Placing your sever behind a firewall
- Disabling non-critical services
- Disabling unused TCP and UDP ports
- Applying all security patches

## Secure Your Server With SSL

Implement Secure Sockets Layer (SSL) to secure all Lumension Endpoint Management and Security Suite (Lumension EMSS) communication.

SSL is a protocol used to secure data transmitted over the Internet. SSL support is included in Web browsers, Web servers, and operating systems so that any type of agent and server can use authenticated and encrypted communications over private and public networks. Lumension EMSS uses SSL when downloading vulnerability data and packages from the Global Subscription Server. SSL is used for transmitting data between the Lumension EMSS Server and Lumension EMSS Agents by enabling SSL during the installation of Lumension EMSS. The installation process requires obtaining a SSL certificate (`.CER`). For details regarding installing with SSL enabled, refer to the *Lumension Endpoint Management and Security Suite 7.1 Server Installation Guide* (*http://portal.lumension.com*).

## Use Secure Passwords

When setting passwords for Lumension Endpoint Management and Security Suite, using secure passwords significantly lowers the probability that your server can be compromised.

Worm attacks, which attempt to install malicious software on a target endpoint, frequently test log ins with weak and commonly used passwords. For secure passwords, Lumension recommends a 12 character password that combines mixed-case alpha characters, numeric characters, and punctuation characters.

## Disabling File and Printer Sharing

When installing Lumension Endpoint Management and Security Suite, you should disable the File and Printer Sharing for Microsoft Networks protocol on the target server. If this protocol is left active, it creates a security risk that intruders can exploit: a Windows networking share. Therefore, File and Printer Sharing for Microsoft Networks should be disabled.

### Disabling File and Printer Sharing in Windows Server 2003

Disable File and Printer Sharing for Microsoft Networks on the Lumension Endpoint Management and Security Suite server, as this protocol is an unnecessary security liability. This protocol is not necessary for your server to function properly.

Disable this protocol from Windows ***Control Panel***.

1. Select **Start** > **Control Panel**.

   **Step Result:** ***Control Panel*** opens.

2. Double-click **Network Connections**.
3. Double-click the applicable **Local Area Connection**.

   **Step Result:** The ***Local Area Connection Status*** dialog opens.

4. Click **Properties**.

   **Step Result:** The ***Local Area Connection Properties*** dialog opens.

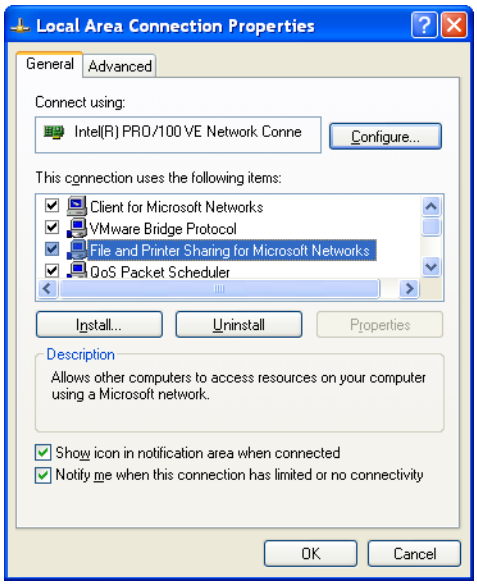



Figure 113: Local Area Connection Properties

5. Clear the check box associated with **File and Printer Sharing for Microsoft Networks**.

   **Caution:** Do not disable **Client for Microsoft Networks**. It is required by both Microsoft SQL Server and Internet Information Server.

6. Click **OK**.

**Result:** File and Printer Sharing for Microsoft Networks is disabled.

## Disabling File and Printer Sharing in Windows Server 2008

Disable File Sharing and Printer Sharing on the Lumension Endpoint Management and Security Suite server, as this protocol is an unnecessary security liability. These protocols are not necessary for your server to function properly.

Disable these protocols from ***Control Panel***.

1. Select **Start** > **Control Panel**.

   **Step Result:** ***Control Panel*** opens.

2. Double-click **Network and Sharing Center**.

   **Step Result:** The ***Network and Sharing Center*** opens.

3. Ensure **File Sharing** is set to **Off**.
4. Ensure **Printer Sharing** is set to **Off**.

5. Close ***Network and Sharing Center***.

**Result:** File Sharing and Printer Sharing are disabled.

## Placing Your Server Behind a Firewall

Lumension recommends placing your Lumension Endpoint Management and Security Suite server behind a firewall. This measurement is considered best-practice.

Since the Lumension Endpoint Management and Security Suite server receives content updates from the Global Subscription Server (GSS), allowing the Lumension Endpoint Management and Security Suite server Internet access is unnecessary. However, access to the GSS must be specified in your firewall configuration.

## Disable Non-Critical Services

Lumension Endpoint Management and Security Suite only requires several essential services to operate. Disabling services that are not critical to its operation reduces security risks.

The default installation of Microsoft Windows sets most features and services to active. Therefore, there are a number of services that can be disabled (e.g.: RPC, Remote Registry, etc.) to reduce security compromises. Although Lumension does not encourage this type of lock down, it can be an effective method to reduce the risk of hacker attacks. The following services are required to run Lumension Endpoint Management and Security Suite:

- World Wide Web Publishing Service
- IIS Admin Service
- SQL Server
- Replication Service
- STATEngine

## Lock Down Unused TCP and UDP Ports

Unused ports pose a security risk to Lumension Endpoint Management and Security Suite servers that operate on the Windows Server 2003 platform. Therefore, these ports should be closed.

Use a firewall to prevent network traffic on various unused and vulnerable TCP and UDP ports. However, if a firewall is not available or additional server-level disablement is desired, TCP and UDP ports can be disabled as a function of the network connection.

**Note:** Ports cannot be closed from the ***Local Area Connection Properties*** dialog within Windows Server 2008. Therefore, Lumension does not recommend disabling the firewall when using Lumension Endpoint Management and Security Suite in a Windows Server 2008 environment.

### Disabling Unused Ports in Windows Server 2003

Lock down unused ports when a firewall is not in place on the server.

1. Select **Start** > **Control Panel**.

   **Step Result:** ***Control Panel*** opens.

2. Double-click **Network Connections**.
3. Double-click the applicable **Local Area Connection**.
4. Ensure the ***General*** tab is selected.
5. Click **Properties**.

   **Step Result:** The ***Local Area Connection Properties*** dialog opens.

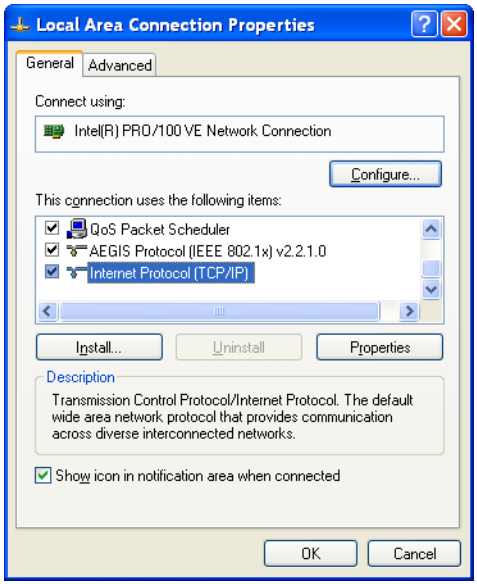



Figure 114: Local Area Connection Properties Dialog

6. Select the **Internet Protocol (TCP/IP)** protocol.

7. Click **Properties**.

   **Step Result:** The ***Internet Protocol (TCP/IP) Properties*** window opens.

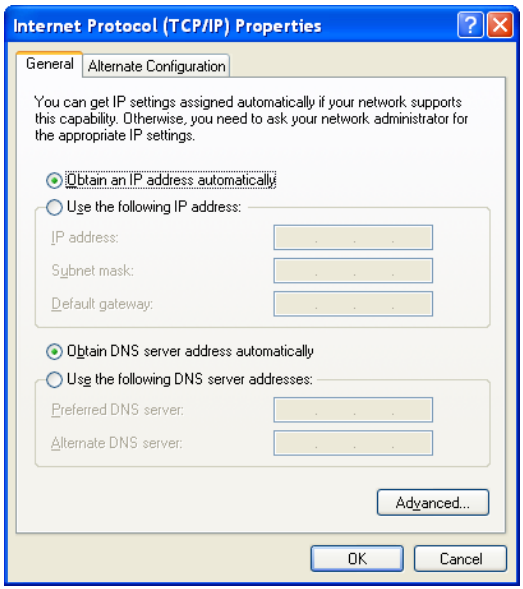

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 115: Internet Protocol (TCP/IP) Properties

8. In the ***General*** tab, click **Advanced**.

   **Step Result:** The ***Advanced TCP/IP Settings*** window opens.

9. Select the ***Options*** tab.
10. Select **TCP/IP Filtering**.

**11.** Click **Properties**.

**Step Result:** The ***TCP/IP Filtering*** window opens.

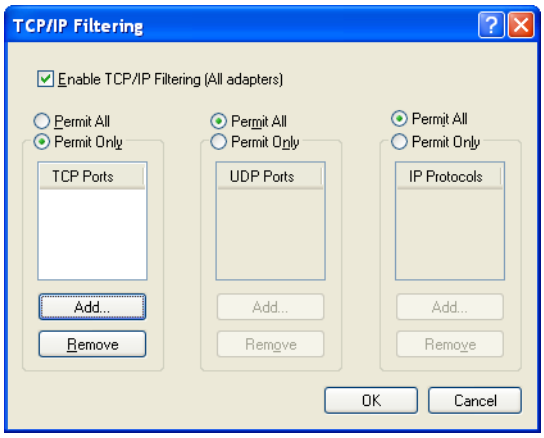



Figure 116: TCP/IP Filtering

**12.** Enable the **Enable TCP/IP Filtering (All Adapters)** option.

**13.** Select the **Permit Only TCP Ports** option.

**14.** Add TCP ports `443` and `80` to the listing of permitted ports.

a) Click **Add**.

**Step Result:** The ***Add Filter*** window opens.

b) Type `443` in the **TCP Port** field.

c) Click **OK**.

**Step Result:** The ***Add Filter*** window closes.

d) Repeat steps a, b, and c to add port `80`.

**Note:** No other ports are required, although you may want to enable additional ports to allow DNS, TS, or VNC.

**15.** Select the **Permit Only UDP Ports** option, leaving the UDP Ports window blank since no UDP ports are required.

**16.** Click **OK**.

**17.** Close the open windows.

**After Completing This Task:**

Since all ports are disabled (except for ports 80 and 443), it will be necessary to add entries to your proxy or `HOSTS` file for the necessary Lumension Web sites and the Global Subscription Server.

## Apply All Security Patches

The Lumension Endpoint Management and Security Suite server should have the most recent security patches installed.

Apply all applicable Microsoft Security Patches to ensure that the server remains protected against all known security threats. Be sure to apply the most recent patches for Internet Information Services, SQL Server, and the version of Windows server in use.

# Appendix
# C

# Configuring the Server and Endpoints for Agent Management Jobs

**In this appendix:**


- Configuring the Scanning System
- Configuring Pre-Windows Vista Endpoint for Discovery
- Configuring Endpoints for Agent Management Jobs (Pre-Windows Vista)
- Configuring Post-Windows Vista Endpoints for Discovery
- Configuring Endpoints for Agent Management Jobs (Post-Windows Vista)
- Troubleshooting Agent Management Jobs


After installing Lumension Endpoint Management and Security Suite on a server, you must perform additional configuration on the endpoints that you want to manage so that agent management jobs will complete successfully.

## Configuring the Scanning System

The Lumension Endpoint Management and Security Suite server must be configured in the following manner so that you can run agent management jobs on your managed endpoints.

1. Click **Start** > **Run**.
2. Enter `regedit` in the **Open** field.
3. Click **OK**.

   **Step Result:** The registry editor displays.

4. In the registry editor, navigate to `HKEY_LOCAL_MACHINE\SYSTEM\Currentcontrolset\Control\Lsa`.

5. Verify that the value for the `lmcompatibilitylevel` registry key is set to 3.

**Note:** Under most network conditions, a setting of 3 is sufficient. However, in some networks, this key may require a different value. To determine which value to use, refer to *http://support.microsoft.com/kb/239869*.

## Configuring Pre-Windows Vista Endpoint for Discovery

For pre-Windows Vista endpoints behind local firewalls, certain ports must be opened in order for them to be discovered. Pre-Windows Vista endpoints that do not have local firewalls in place will be discovered without performing this procedure.

Perform this task from the pre-Windows Vista endpoint your are configuring for discovery.

1. Select **Start** > **Control Panel**.

   **Step Result:** ***Control Panel*** opens.

2. Double-click **Windows Firewall**.

   **Step Result:** The ***Windows Firewall*** dialog opens.

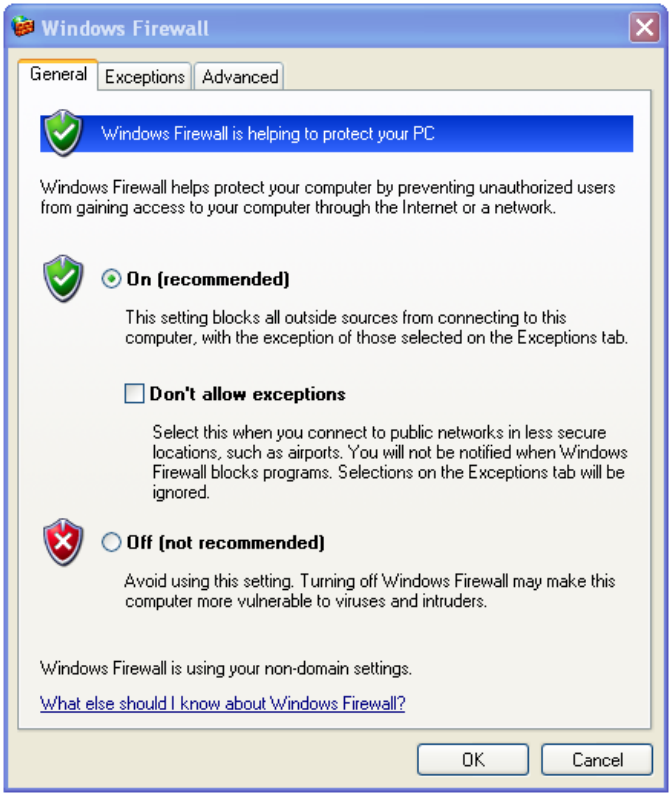

Windows Firewall
General
Exceptions
Advanced
Windows Firewall is helping to protect your PC
Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.
On (recommended)
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.
Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.
Windows Firewall is using your non-domain settings.
What else should I know about Windows Firewall?
OK
Cancel

Figure 117: Windows Firewall Dialog

3. Select the ***Exceptions*** tab.

**Step Result:**

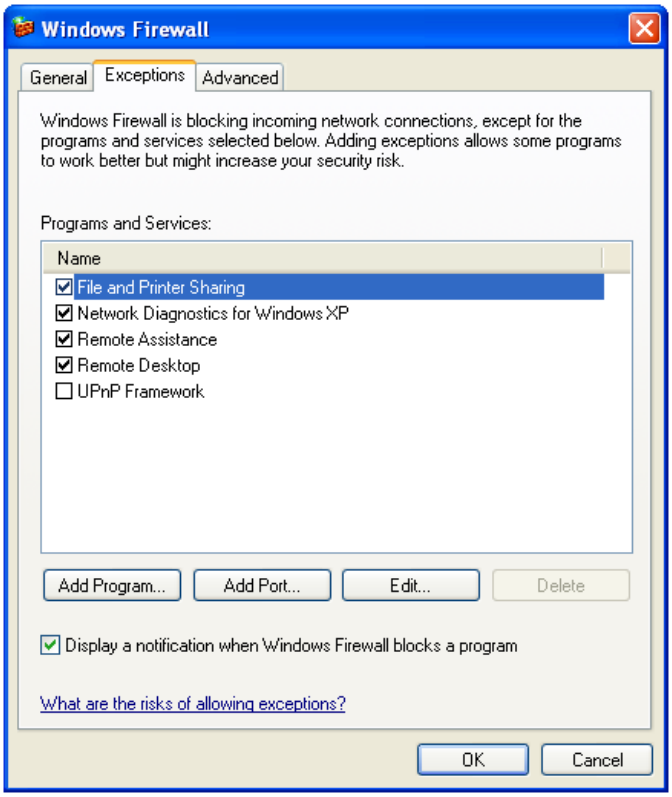



Figure 118: Exceptions Tab

4. Ensure the **File and Printer Sharing** check box is selected.

   A **File and Printer Sharing** exception opens the following ports, which are essential for discovery and agent management.

   - 445/TCP
   - 139/TCP
   - 135/UDP
   - 137/UDP

5. Click **OK**.

**Result:** The endpoint can now be discovered during discovery scan jobs and agent management jobs.

# Configuring Endpoints for Agent Management Jobs (Pre-Windows Vista)

In order to successfully perform network-based assessments, you must complete the following configuration procedure on your managed endpoints after you install the Lumension Endpoint Management and Security Suite Agent.

Configure your networked endpoints running pre-Windows Vista operating systems (Windows 2003, Windows XP, and so on) according the following procedure.

1. Select **Start** > **Run**.
2. Enter `cmd` in the **Open** field.
3. Click **OK**.

   **Step Result:** The command prompt displays.

4. Type `net share` and press ENTER.
5. Verify that C$ and ADMIN$ are enabled and appear in the `Share name` column.

   If they are not, type the following commands to enable these shares.

   - `NET SHARE C$=C`
   - `NET SHARE ADMIN$`

   These commands enable the shares until the system reboots.

6. Select **Start** > **Control Panel**.

   **Step Result:** ***Control Panel*** opens.

7. Double-click **Administrative Tools**.

   **Step Result:** The ***Administrative Tools*** dialog opens.

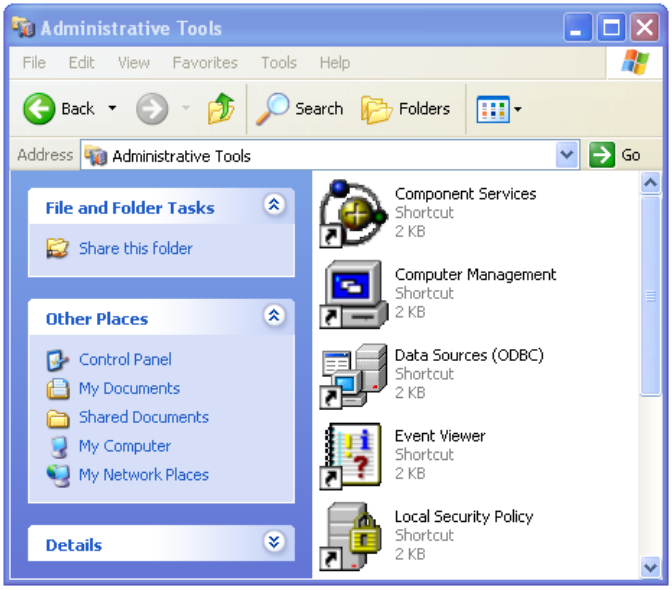



Figure 119: Administrative Tools Dialog

8. Double-click **Services**.

   **Step Result:** The ***Services*** dialog opens.

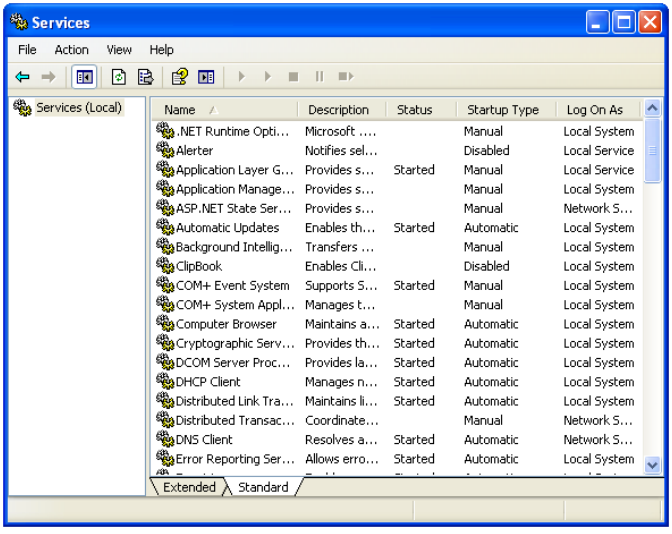

Services
File Action View Help
Services (Local)
Name Description Status Startup Type Log On As
.NET Runtime Opti... Microsoft .... Manual Local System
Alerter Notifies sel... Disabled Local Service
Application Layer G... Provides s... Started Manual Local Service
Application Manage... Provides s... Manual Local System
ASP.NET State Ser... Provides s... Manual Network S...
Automatic Updates Enables th... Started Automatic Local System
Background Intellig... Transfers ... Manual Local System
ClipBook Enables Cli... Disabled Local System
COM+ Event System Supports S... Started Manual Local System
COM+ System Appl... Manages t... Manual Local System
Computer Browser Maintains a... Started Automatic Local System
Cryptographic Serv... Provides th... Started Automatic Local System
DCOM Server Proc... Provides la... Started Automatic Local System
DHCP Client Manages n... Started Automatic Local System
Distributed Link Tra... Maintains li... Started Automatic Local System
Distributed Transac... Coordinate... Manual Network S...
DNS Client Resolves a... Started Automatic Network S...
Error Reporting Ser... Allows erro... Started Automatic Local System
Extended Standard

Figure 120: Services Dialog

9. Verify that the following services are running:

   - DCOM Server Process Launcher
   - Remote Procedure Call (RPC)
   - Remote Registry
   - Server
   - Windows Firewall/Internet Connection Sharing
   - Windows Management Instrumentation

   If any of these services is not running, start it by completing the following substeps.

   a) Double-click the applicable service.
   b) Ensure the ***General*** tab is selected.
   c) From the **Startup type** list, select **Automatic**.
   d) Click **Start**.
   e) Click **OK**.

10. Select **Start** > **Run**.
11. Enter `gpedit.msc` in the **Open** field.
12. Click **OK**.

    **Step Result:** The ***Group Policy*** dialog opens.

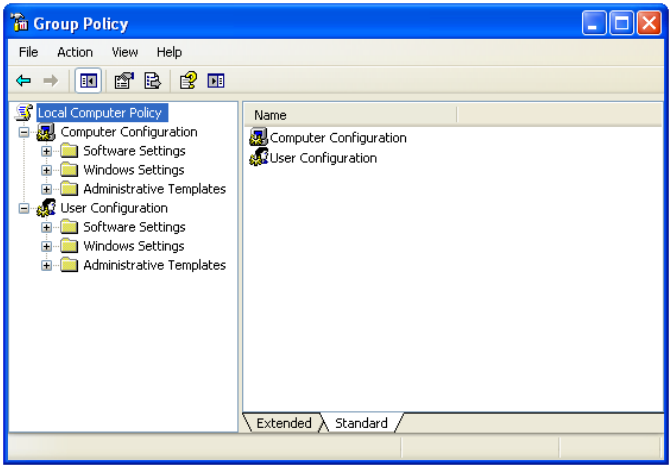



Figure 121: Services Dialog

13. Expand the directory tree structure to **Computer Configuration** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall** > **Domain Profile/Standard Profiles**.

    The standard profile is enforced for workgroup members, and the domain profile is enforced for domain members. Edit both lists for consistency.

**14.** Edit the following settings according to the following table.

| Value | Setting |
|---|---|
| **Enable** | • **Windows Firewall: Allow file and printer sharing exception**<br>• **Windows Firewall: Allow remote administration exception** |
| **Disable** | • **Windows Firewall: Do not allow exceptions** |

To edit these settings, perform the following substeps.

a) Right-click the applicable setting.
b) Select **Properties**.
c) Select the applicable option (**Enable** or **Disable**).
d) If desired, define an IP range in the **Allow unsolicited incoming messages from** field.

> **Note:** This substep is only applicable to the **Windows Firewall: Allow file and printer sharing exception** and **Windows Firewall: Allow remote administration exception** settings. To define a range, you may use the following syntax: `*` (any IP address), `10.3.2.0/24` (specific Class C subnet), and `localsubnet` (for local subnetwork access only).
>
> This input is not validated. By default, you should leave the box blank to allow any IP address.

e) Click **OK**.

**15.** Select **Start** > **Run**.

**16.** Enter `regedit` in the **Open** field.

**17.** Click **OK**.

**Step Result:** The ***Registry Editor*** opens.

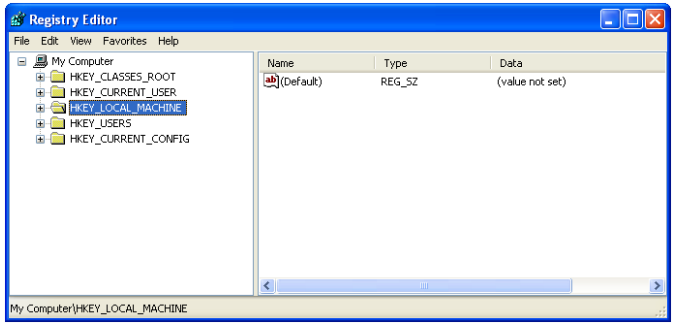



Figure 122: Services Dialog

**18.** From the directory tree structure, expand to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.

**19.** Verify that the value for the `lmcompatibilitylevel` registry key is set to 3 or 5.

If the key is not set to one of the following values, complete the following substeps.

**Note:** Under most network conditions, a setting of 3 or 5 is sufficient. However, in some networks, this key may require a different value. To determine which value to use, refer to *How to enable NTLM 2 authentication* (*http://support.microsoft.com/kb/239869*).

a) Double-click **lmcompatibilitylevel**.

**Step Result:** The ***Edit DWORD Value*** dialog opens.

b) In the **Value data** field, type 3 or 5 (unless another value is required).

c) Click **OK**.

**20.** Select **Start** > **Run**.

**21.** Enter `cmd` in the **Open** field.

**22.** Click **OK**.

**Step Result:** A command prompt displays.

**23.** Type `gpupdate /force` and press ENTER.

**24.** Select **Start** > **Control Panel**.

**Step Result:** ***Control Panel*** opens.

**25.** Double-click **Network Connections**.

**Step Result:** The ***Network Connections*** dialog opens.

**26.** Right-click your local area connection.

**27.** Select **Properties**.

**Step Result:** The ***Local Area Connection Properties*** dialog opens.

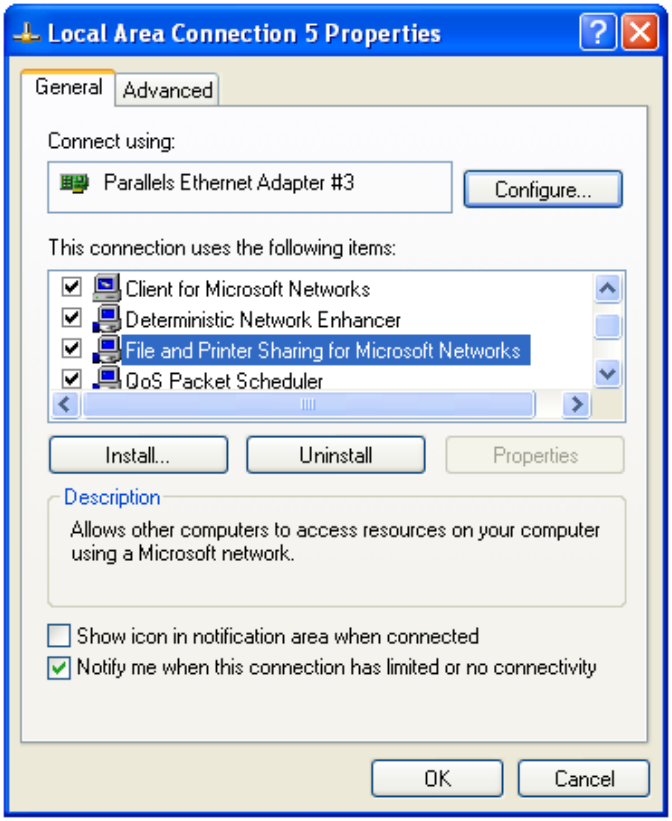



Figure 123: Local Area Connection Properties Dialog

**28.** Ensure the **File and Printer Sharing for Microsoft Networks** check box is selected.

**29.** Click **OK**.

## Configuring Post-Windows Vista Endpoints for Discovery

For Lumension Endpoint Management and Security Suite to discover Windows Vista, Windows Server 2008, and Windows 7 endpoints during discovery scan jobs and agent management jobs, they must have both network discovery and file sharing enabled. Target endpoints without these features enabled will not be discovered.

Perform these steps on the applicable post-Windows Vista endpoint.

**Note:** The following steps were created using Windows Vista. When configuring Windows Server 2008 or Windows 7 for agent management jobs, steps may differ slightly.

1. Select **Start** > **Control Panel**.

   **Step Result:** ***Control Panel*** opens.

   **Note:** Instructions for navigating within ***Control Panel*** assume the default view is selected.

2. Click **System and Security**.

   **Step Result:** The ***System and Security*** dialog opens.

3. Click **Administrative Tools**.

   **Step Result:** The ***Administrative Tools*** dialog opens.

4. Double-click **Services**.

   **Step Result:** The ***Services*** dialog opens.

5. Ensure the following services are started:

   - DNS Client
   - Function Discovery Research Publication
   - SSDP Discvoery
   - UPnP Device Discovery

   Enable any unstarted services by completing the following substeps:

   a) Right-click the applicable service.
   b) Select **Start**.

6. Select **Start** > **Control Panel**.

   **Step Result:** ***Control Panel*** opens.

7. Click **Network and Internet**.

   **Step Result:** The ***Network and Internet*** dialog opens.

8. Click **Network and Sharing Center**.
9. Ensure **Network discovery** is enabled.

   Based on the endpoint operating system, complete the applicable substeps that follow.

| Operating System | Substep |
|---|---|
| **For Windows Vista and Windows Server 2008:** | **1.** Click the arrow icon adjacent to **Network discovery**.<br>**2.** Ensure the **Turn on network discovery** option is selected.<br>**3.** Click **Apply**. |

| Operating System | Substep |
|---|---|
| **For Windows 7:** | 1. Click **Change advanced sharing settings**.<br>2. Scroll to **Network discovery**.<br>3. Ensure the **Turn on network discovery** option is selected.<br>4. Click **Save Changes**. |

10. Select **Start** > **Control Panel**.

    **Step Result:** ***Control Panel*** opens.

11. Click **Network and Internet**.

    **Step Result:** The ***Network and Internet*** dialog opens.

12. Open the ***Windows Firewall*** dialog.

    Based on the endpoint operating system, complete the applicable set of substeps.

| Operating System | Substeps |
|---|---|
| **For Windows Vista and Windows Server 2008:** | 1. Click **Windows Firewall**.<br>2. Click the **Change Settings** link.<br>3. Select the ***Exceptions*** tab.<br>4. Ensure the **File and Printer Sharing** check box is selected.<br>A **File and Printer Sharing** exception opens the following ports, which are essential for discovery and agent management.<br>• 445/TCP<br>• 139/TCP<br>• 135/UDP<br>• 137/UDP<br>5. Click **OK**. |

| Operating System | Substeps |
|---|---|
| **For Windows 7:** | 1. Click **Network and Sharing Center**.<br>2. Click **Windows Firewall**.<br>3. Click **Allow a program or feature through Windows Firewall**.<br>4. Select the **File and Printer Sharing** check box.<br>Selecting this option opens the following ports, which are essential for discovery and agent management.<br>• 445/TCP<br>• 139/TCP<br>• 135/UDP<br>• 137/UDP<br>5. Click **OK**. |

**Result:** **Network discovery** and **File sharing** are enabled, and the ports are opened. The endpoint can now be discovered during discovery scan jobs and agent management jobs.

## Configuring Endpoints for Agent Management Jobs (Post-Windows Vista)

In order to successfully perform network-based assessments, you must complete the following configuration procedure on your managed endpoints before you install the agent.

**Prerequisites:**

Complete *Configuring Post-Windows Vista Endpoints for Discovery* on page 331.

Configure your networked endpoints running Windows Vista, Windows Server 2008, or Windows 7 according the following procedure.

**Note:** While executing some of the following steps, a ***User Account Control*** dialog may appear, to verify permission to continue with the requested action. Click **Continue** and proceed to the next step.

1. Open a run prompt.

   Follow the substeps associated with the applicable operating system.

| Operating System | Steps |
|---|---|
| **To open a run prompt in Windows Vista or Windows Server 2008:** | Select **Start** > **Run**. |

| Operating System | Steps |
|---|---|
| **To open a run prompt in Windows 7:** | 1. Select the **Start** menu.<br>2. Enter `run` in the **Search programs and files** field. |

2. Enter `cmd` in the **Open** field.
3. Click **OK**.

   **Step Result:** The command prompt displays.

4. Type `net share` and press ENTER.
5. Verify that C$ and ADMIN$ are enabled and appear in the `Share name` column.
   If they are not, type the following commands to enable these shares.

   - `NET SHARE C$=C`
   - `NET SHARE ADMIN$`

   These commands enable the shares until the system reboots.
6. Select **Start** > **Control Panel**.

   **Step Result:** ***Control Panel*** opens.

   **Note:** Instructions for navigating within ***Control Panel*** assume the default view is selected.

7. Click **System and Security**.

   **Step Result:** The ***System and Security*** dialog opens.

8. Click **Administrative Tools**.

   **Step Result:** The ***Administrative Tools*** dialog opens.

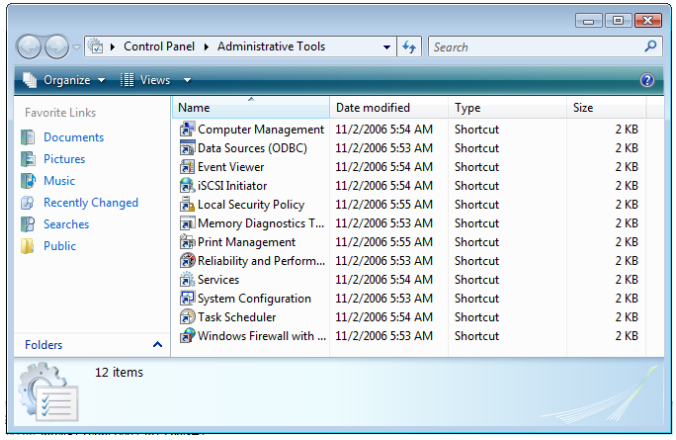

Control Panel ▸ Administrative Tools
Search
Organize
Views
Favorite Links
Documents
Pictures
Music
Recently Changed
Searches
Public
Folders
Name
Date modified
Type
Size
Computer Management 11/2/2006 5:54 AM Shortcut 2 KB
Data Sources (ODBC) 11/2/2006 5:53 AM Shortcut 2 KB
Event Viewer 11/2/2006 5:54 AM Shortcut 2 KB
iSCSI Initiator 11/2/2006 5:54 AM Shortcut 2 KB
Local Security Policy 11/2/2006 5:55 AM Shortcut 2 KB
Memory Diagnostics T... 11/2/2006 5:53 AM Shortcut 2 KB
Print Management 11/2/2006 5:55 AM Shortcut 2 KB
Reliability and Perform... 11/2/2006 5:53 AM Shortcut 2 KB
Services 11/2/2006 5:54 AM Shortcut 2 KB
System Configuration 11/2/2006 5:53 AM Shortcut 2 KB
Task Scheduler 11/2/2006 5:54 AM Shortcut 2 KB
Windows Firewall with ... 11/2/2006 5:53 AM Shortcut 2 KB
12 items

Figure 124: Administrative Tools Dialog

**9.** Double-click **Services**.

**Step Result:** The ***Services*** dialog opens.

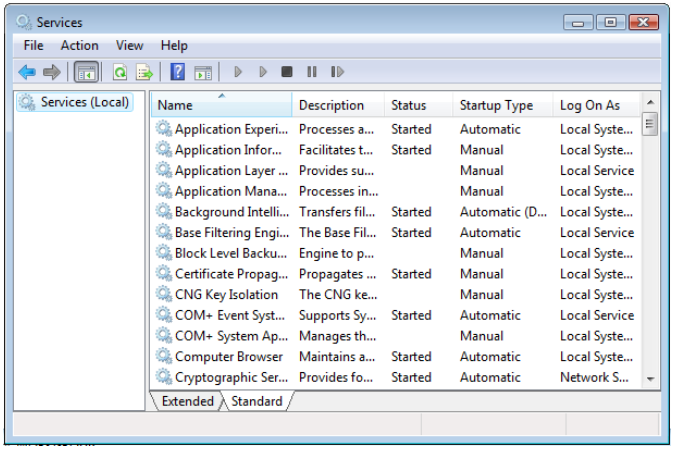

Services
File Action View Help
Services (Local)
Name Description Status Startup Type Log On As
Application Experi... Processes a... Started Automatic Local Syste...
Application Infor... Facilitates t... Started Manual Local Syste...
Application Layer ... Provides su... Manual Local Service
Application Mana... Processes in... Manual Local Syste...
Background Intelli... Transfers fil... Started Automatic (D... Local Syste...
Base Filtering Engi... The Base Fil... Started Automatic Local Service
Block Level Backu... Engine to p... Manual Local Syste...
Certificate Propag... Propagates ... Started Manual Local Syste...
CNG Key Isolation The CNG ke... Manual Local Syste...
COM+ Event Syst... Supports Sy... Started Automatic Local Service
COM+ System Ap... Manages th... Manual Local Syste...
Computer Browser Maintains a... Started Automatic Local Syste...
Cryptographic Ser... Provides fo... Started Automatic Network S...
Extended Standard

Figure 125: Services Dialog

**10.** Verify that the following services are running:

- DCOM Server Process Launcher
- Remote Procedure Call (RPC)
- Remote Registry
- Server
- Windows Firewall/Internet Connection Sharing
- Windows Management Instrumentation

If any of these services is not running, start it by completing the following substeps.

a) Double-click the applicable service.
b) Ensure the ***General*** tab is selected.
c) From the **Startup type** list, select **Automatic**.
d) Click **Start**.
e) Click **OK**.

**11.** Open a run prompt.

Follow the substeps associated with the applicable operating system.

| Operating System | Steps |
|---|---|
| **To open a run prompt in Windows Vista or Windows Server 2008:** | Select **Start** > **Run**. |

| Operating System | Steps |
|---|---|
| **To open a run prompt in Windows 7:** | 1. Select the **Start** menu.<br>2. Enter `run` in the **Search programs and files** field. |

12. Enter `gpedit.msc` in the **Open** field.
13. Click **OK**.

    **Step Result:** The ***Group Policy Object Editor*** opens.

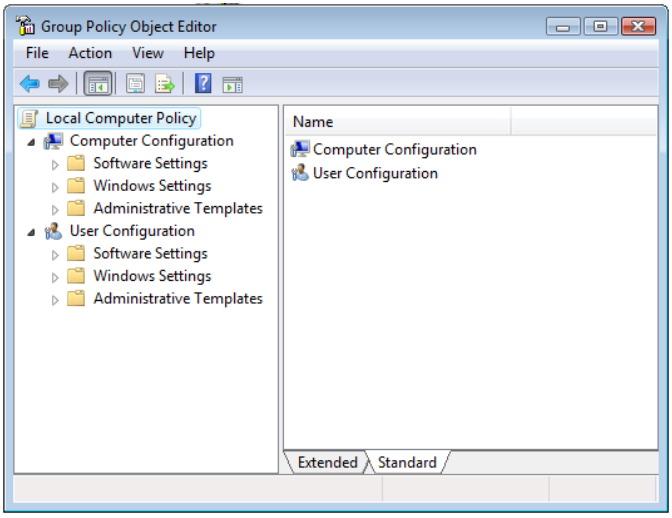



Figure 126: Group Policy Object Editor

> **Note:** In Windows 7, this dialog is entitled the ***Local Group Policy Editor***.

14. Expand the directory tree structure to **Computer Configuration** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall** > **Domain Profile/Standard Profiles**.

    The standard profile is enforced for workgroup members, and the domain profile is enforced for domain members. Edit both lists for consistency.

**15.** Edit the following settings according to the following table.

| Value | Setting |
|---|---|
| **Enable** | • **Windows Firewall: Allow file and printer sharing exception**<br>• **Windows Firewall: Allow remote administration exception**<br>• **Windows Firewall: Allow ICMP exceptions** |
| **Disable** | • **Windows Firewall: Do not allow exceptions** |

To edit these settings, perform the following substeps.

a) Right-click the applicable setting.
b) Select **Properties**.
c) Select the applicable option (**Enable** or **Disable**).

> **Note:** After enabling the **Windows Firewall: Allow ICMP exceptions** setting, select the **Allow inbound echo request** check box. Ensure all other check boxes are clear.

d) If desired, define an IP range in the **Allow unsolicited incoming messages from** field.

> **Note:** This substep is only applicable to the **Windows Firewall: Allow file and printer sharing exception** and **Windows Firewall: Allow remote administration exception** settings. To define a range, you may use the following syntax: `*` (any IP address), `10.3.2.0/24` (specific Class C subnet), and `localsubnet` (for local subnetwork access only).
>
> This input is not validated. By default, you should leave the box blank to allow any IP address.

e) Click **OK**.

**16.** Open a run prompt.

Follow the substeps associated with the applicable operating system.

| Operating System | Steps |
|---|---|
| **To open a run prompt in Windows Vista or Windows Server 2008:** | Select **Start** > **Run**. |
| **To open a run prompt in Windows 7:** | **1.** Select the **Start** menu.<br>**2.** Enter `run` in the **Search programs and files** field. |

**17.** Enter `regedit` in the **Open** field.

**18.** Click **OK**.

**Step Result:** The ***Registry Editor*** displays.

19. From the directory tree structure, expand to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.
20. Verify that the value for the `lmcompatibilitylevel` registry key is set to 3 or 5.

    If the key is not set to one of the following values, complete the following substeps.

    **Note:** Under most network conditions, a setting of 3 or 5 is sufficient. However, in some networks, this key may require a different value. To determine which value to use, refer to *How to enable NTLM 2 authentication* (*http://support.microsoft.com/kb/239869*).

    a) Double-click **lmcompatibilitylevel**.

    **Step Result:** The ***Edit DWORD Value*** dialog opens.

    b) In the **Value data** field, type 3 or 5 (unless another value is required).
    c) Click **OK**.
21. Open a run prompt.

    Follow the substeps associated with the applicable operating system.

| Operating System | Steps |
|---|---|
| **To open a run prompt in Windows Vista or Windows Server 2008:** | Select **Start** > **Run**. |
| **To open a run prompt in Windows 7:** | 1. Select the **Start** menu.<br>2. Enter `run` in the **Search programs and files** field. |

22. Enter `cmd` in the **Open** field.
23. Click **OK**.

    **Step Result:** A command prompt displays.
24. Type `gpupdate /force` and press ENTER.

## Resolving Endpoint UAC Issues

On endpoints running Windows Vista or later operating systems, UAC security features are set to highly restrictive levels by default. These settings must be configured properly to ensure agent management job success.

When a post-Windows Vista endpoint is in this default UAC configuration, agent management jobs fail with an `access denied` error.

Use one of two methods to resolve this issue:

| | |
|---|---|
| **Add a domain account** | Adding a domain account to the applicable endpoint's local administrator's group will typically resolve the issue. To use this method, add the endpoint to a domain (provided it isn't already added), and then add a domain user to the endpoint's local administrator group. Running an agent management job configured to use this domain account's credentials will allow the job to complete successfully.<br>**Note:** The domain account added to the local administrator's group *must* be an individual domain account; you cannot add a domain group. |
| **Set a Registry Value** | If the user of a local administrative account is desired or required, you can set a registry value to resolve this issue.<br>Create a `DWORD` registry value named *LocalAccountTokenFilterPolicy* in the `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\` registry hive. Set its value to *1*.<br>No reboot is required. This method allows a local administrative account to successfully run agent management jobs.<br>**Note:** For additional information about this method, refer to *http://support.microsoft.com/kb/942817*. |

## Troubleshooting Agent Management Jobs

If agent managements are not completing successfully, additional configuration may be required.

If the Lumension Endpoint Management and Security Suite server or an applicable network endpoint has lost its trust relationship with the domain, agent management jobs will fail with an error of `access denied`.

To verify if this issue is causing agent management job failure, ensure that the Lumension EMSS server can connect to the applicable endpoints C$, and that the applicable endpoints can connect to the server's C$. To verify these connections, type the following command from the applicable endpoint or server prompt: `\\EndpointIPAddress\C$`.

If the following system output results from the command, your endpoint or server has lost its trust relationship with the domain: `The trust relationship between this workstation and the primary domain failed.`

To resolve this issue, remove the applicable server or endpoint from the domain, and then add it back. This process forces the domain to refresh the endpoint password. The endpoint password prompts users for resetting at scheduled intervals according to its security settings.

To disable password changes, complete *Disabling Password Changes* on page 341.

## Disabling Password Changes

Do disable password changes, create a registry key for the applicable endpoint.

Perform this task from the applicable endpoint.

1. Select **Start** > **Run**.

   **Step Result:** The ***Run*** dialog opens.

2. Type `regedit` in the **Open** field.
3. Click **OK**.

   **Step Result:** The ***Registry Editor*** opens.

4. Expand the directory tree structure to `My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`.
5. Right-click `DisablePasswordChange`.
6. Select **Modify**.

   **Step Result:** The ***Edit DWORD Value*** dialog opens.

7. In the **Value data** field, type `1`.
8. Click **OK**.

**Result:** The key value is updated. User profile passwords can no longer be edited on the applicable endpoint.

# Appendix
# D

# Creating a Disaster Recovery Solution

**In this appendix:**


- Preparing Your Database
- Creating a Manual Solution
- Creating an Automated Solution


Lumension Endpoint Management and Security Suite uses Microsoft SQL Server to store data values; therefore, you should prepare your instance of Microsoft SQL Server for a disaster.

The most important part of an effective disaster recovery solution is having a current and valid backup. You can create backups either manually or as part of a Database Maintenance Plan.

**Note:** This appendix applies to Microsoft SQL Server 2008 and requires the Microsoft SQL Server Management Studio. The Management Studio is available by upgrading to SQL Server 2008 Standard or Enterprise. For further information, see *Microsoft SQL Server 2008* (*http://www.microsoft.com/sqlserver/2008/en/us/default.aspx*).

## Preparing Your Database

In the event of a disaster, detailed transaction logs are useful when restoring your database. You can control the level of detail that your logs record.

The installation of Lumension Endpoint Management and Security Suite sets your database to a recovery model of `Simple`. To use *Transaction Logs*, and thus increase the quality of your disaster recovery solution, you should change the recovery model to `Full`.

### Changing the Database Recovery Model

Modify the database recovery model to record more robust details about the events leading to a disaster.

Database recovery model edits take place in the ***SQL Server Management Studio***.

1. Open the ***Microsoft SQL Server Management Studio*** (**Start** > **All Programs** > **Microsoft SQL Server 2008** > **SQL Server Management Studio**).
2. Log into your database server.
3. In the directory tree, expand ***Server Name\SQL Instance*** > **Databases**.
4. Right-click the `PLUS` database.

5. Select **Properties**.

   **Step Result:** The ***Database Properties*** window opens.

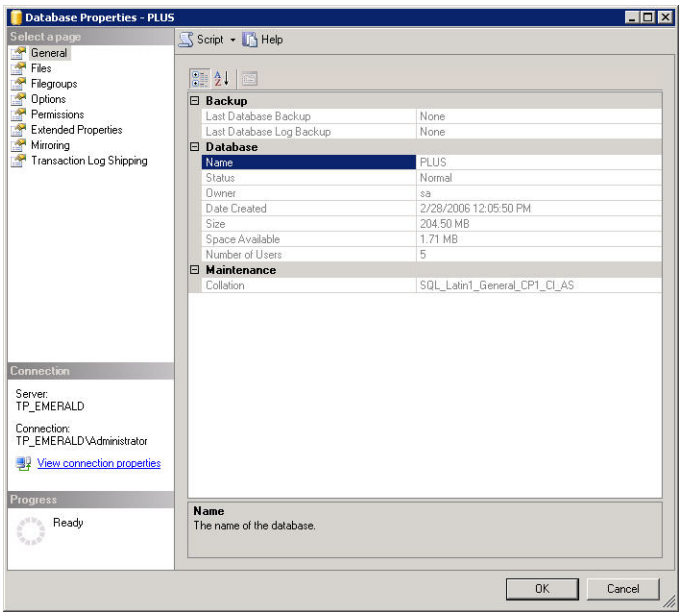



Figure 127: Database Properties

6. In the **Select a Page** pane, click **Options**.

   **Step Result:** The ***Options*** page opens.

7. In the **Recovery model** list, select **Full**.
8. Click **OK**.

   **Step Result:** The changes are saved and the ***Database Properties*** window closes.

9. Repeat the recovery model modification process for the following databases:

   - `PLUS_Staging`
   - `UPCCommon`
   - `SCM`
   - `STAT_Guardian`
   - `PLUS_Reports` (if exists)

**After Completing This Task:**

You must create a backup of each database before any Transaction logs will be created. Refer to *Creating a Database Backup* on page 345 to create a one-time backup of your database.

# Creating a Manual Solution

To prevent data loss, create a database solution, and implement it in the event of a disaster.

While a Maintenance Plan will allow you to automate the backup of your databases and transaction logs, you can also create and restore individual backups using the SQL Server Management Studio.

## Creating a Database Backup

The most important part of an effective disaster recovery technique is having a current and valid backup. Create a backup for the SQL Server instance associated with Lumension Endpoint Management and Security Suite to assure minimal system data is lost if a disaster occurs.

Backups are created within SQL Server Management Studio.

1. Open the ***Microsoft SQL Server Management Studio*** (**Start** > **Programs** > **Microsoft SQL Server 2008** > **SQL Server Management Studio**).
2. Log into your database server.
3. In the directory tree, expand ***Server Name\SQL Instance*** > **Databases**.
4. Right-click the PLUS database.
5. Select **Tasks** > **Backup**.

   **Step Result:** The ***Back Up Database*** window opens.

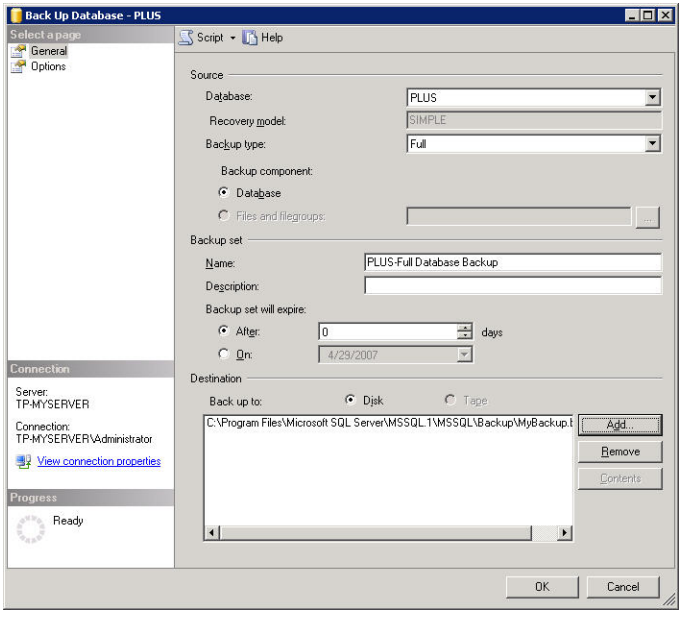



Figure 128: Back Up Database

6. Ensure that the Source values are set as follows:

- **Database**: `PLUS`
- **Recovery model**: `Full`

> **Note:** If the **Recovery model** is not set to Full, refer to *Changing the Database Recovery Model* on page 343.

- **Backup Type**: `Full`
- **Backup Component**: `Database`

7. Define the **Backup set** identification fields.

   The following table describes each field.

| Field | Description |
|---|---|
| **Name** | The name of the backup set. |
| **Description** | The description of the backup set. |

8. Define the backup set expiration date.

   Use one of the following methods.

| Method | Steps |
|---|---|
| **To define an expiration date based on a set number of days:** | 1. Select the **After** option.<br>2. Type the desired number in the **After** field. |
| **To define an expiration date based on a set date:** | 1. Select the **On** option.<br>2. Select the desired date frm the **On** list. |

9. Define your backup **Destination** settings.
   a) Select either the **Disk** or **Tape** option.
   b) Define the destination **Folder**.

> **Note:** For performance reasons, it is recommended that you create your database backup in a directory that is not on the same physical drive as your database.

**10.** Select `Options` within the **Select a page** pane.

**Step Result:** The ***Options*** page displays.

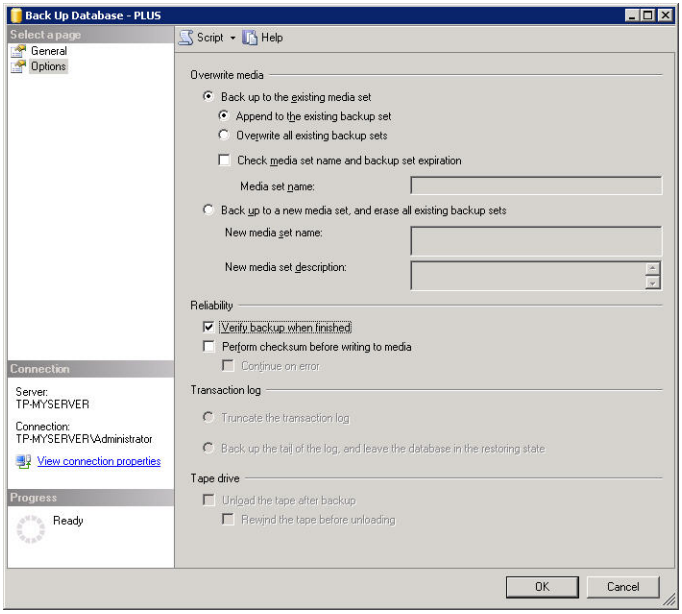



Figure 129: Back Up Database - Options

**11.** Select whether to **Backup up to the existing media set** or **Back up to a new media set, and erase all existing backup sets** as is appropriate for your organization.

**12.** Select the **Verify backup when finished** option to ensure a valid backup.

**13.** Click **OK**.

**14.** Repeat for the following databases:

- `PLUS_Staging`
- `UPCCommon`
- `SCM`
- `STAT_Guardian`
- `PLUS_Reports` (if exists)

## After Completing This Task:

You must also backup the Lumension EMSS content directory.

**Tip:** The default location of the content directory is `<Installation Directory>\Lumension\EMSS\Content`. However, if this directory was modified during installation, you can verify its location by viewing the `\HKEY_LOCAL_MACHINE\SOFTWARE\Patchlink.com\Update\ISAPI\Storage` registry key.

## Restoring a Database Backup

Another important part of an effective Disaster Recovery Solution is having a process defined in which to restore your database backup.

**Prerequisites:**

Prior to restoring the database backup you must install the Lumension Endpoint Management and Security Suite server using the same serial number that was used previously.

**Important:** After installing the Lumension Endpoint Management and Security Suite server do not open the user interface until after you have restored the databases.

1. Open the ***Services Management Console*** (**Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**).
2. Right-click the `World Wide Web Publishing` service.
3. Select **Stop** to stop the `World Wide Web Publishing` (IIS) service.
4. Repeat steps 2 and 3 for the following services:
   - `EDS LanPortal`
   - `EDS MessageBroker`
   - `EDS Server`
   - `Replication Service`
   - `STATEngine`
5. Restore the backup you made of the content directory, over the new content directory (`<Installation Directory>\Lumension\EMSS\Content` by default). However, if this directory was modified during installation, you can verify its location by viewing the `\HKEY_LOCAL_MACHINE\SOFTWARE\Patchlink.com\Update\ISAPI\Storage` registry key.
6. Open the ***Microsoft SQL Server Management Studio*** (**Start** > **Programs** > **Microsoft SQL Server 2008** > **SQL Server Management Studio**).
7. Using an user account that has *sysadmin* rights, log into your database server.
8. In the directory tree, expand ***Server Name\SQL Instance*** **> Databases**.
9. Right-click on the **Databases** folder.

10. Select **Restore Database**

    **Step Result:** The ***Restore Database*** window opens.

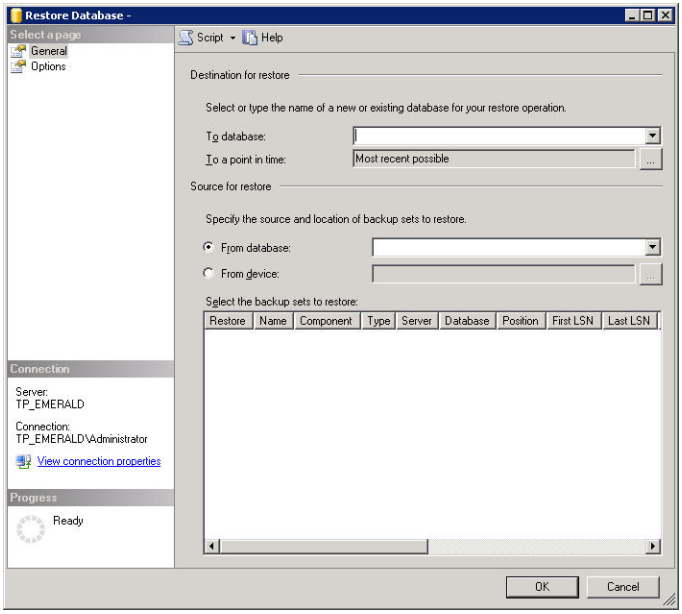



Figure 130: Restore Database

11. In the **To database** field, type or select the `PLUS`database.
12. Select **From device** and click the **Ellipses** button (...).

    **Step Result:** The ***Specify Backup*** dialog opens.

13. Click **Add**.

    **Step Result:** The ***Locate Backup File*** dialog opens.

14. Locate and select your backup (`.bak`) file.
15. Click **OK**.
16. Click **OK** to return to the ***Restore Database*** window.
17. Select the check-box associated with your backup within the **Select the backup sets to restore** table.

**18.** Click `Options` within the **Select a page** pane.

**Step Result:** The ***Options*** page displays.

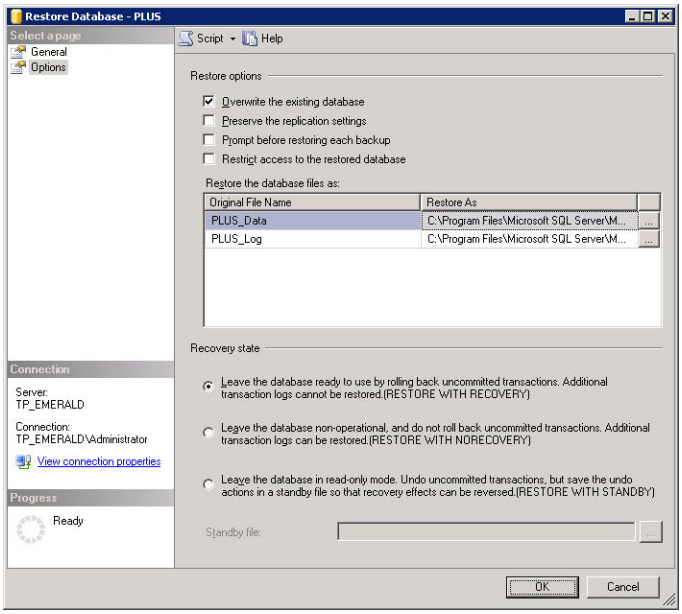

Restore Database - PLUS
Select a page
General
Options
Script
Help
Restore options
Overwrite the existing database
Preserve the replication settings
Prompt before restoring each backup
Restrict access to the restored database
Restore the database files as:
Original File Name
Restore As
PLUS_Data
C:\Program Files\Microsoft SQL Server\M...
PLUS_Log
C:\Program Files\Microsoft SQL Server\M...
Recovery state
Leave the database ready to use by rolling back uncommitted transactions. Additional transaction logs cannot be restored.(RESTORE WITH RECOVERY)
Leave the database non-operational, and do not roll back uncommitted transactions. Additional transaction logs can be restored.(RESTORE WITH NORECOVERY)
Leave the database in read-only mode. Undo uncommitted transactions, but save the undo actions in a standby file so that recovery effects can be reversed.(RESTORE WITH STANDBY)
Standby file:
Connection
Server:
TP_EMERALD
Connection:
TP_EMERALD\Administrator
View connection properties
Progress
Ready
OK
Cancel

Figure 131: Restore Database - Options

**19.** Ensure the **Overwrite the existing database** option is selected.

**20.** Verify, and correct if necessary, the directory path within the **Restore the database files as** table.

**21.** Ensure the **Leave the database ready to use** option is selected.

**22.** Click **OK** to begin the database restoration.

**23.** After the restore is complete run the following SQL command against the database.

```
exec sp_changedbowner 'sa'
```

**24.** Repeat steps 9 through 23, restoring each of the following databases:

- `PLUS_Staging`
- `UPCCommon`
- `SCM`
- `STAT_Guardian`
- `PLUS_Reports` (if exists)

**25.** Against the master database run the following SQL command.

```
exec sp_dboption N'PLUS', N'DB CHAINING', N'true'
exec sp_dboption N'PLUS_Staging', N'DB CHAINING', N'true'
exec sp_dboption N'UPCCommon', N'DB CHAINING', N'true'
exec sp_dboption N'SCM', N'DB CHAINING', N'true'
exec sp_dboption N'STAT_Guardian', N'DB CHAINING', N'true'
```

**26.** If the computer name, Service account name, or Client account name is different you must perform the following steps.

a) Delete the previous Service account and Client account users from **each** database.

b) Add the new Service and Client account users to the following roles for each database.

- `PLUS` - Update Server, aspnet_ChangeNotification_ReceiveNotificationsOnlyAcccess
- `PLUS_Staging` - Update Server
- `SCM` - SCM Server
- `STAT_Guardian` - Guardian_Admin
- `UPCCommon` - UPC Server

**27.** If you re-installed the Lumension EMSS server with a different user name than was used when originally installed, run the following SQL command.

```
UPDATE AccountContacts SET UserName = 'NewUserName' WHERE UserName = 'OldUserName'
```

**28.** If you re-installed the Lumension EMSS server with the content directory in a different location than the original installation, run the following SQL command.

```
UPDATE SystemConfig SET SystemConfig_Value = 'NewStorageSystemPath' WHERE
SystemConfig_Name = 'Storage'
```

**29.** If you re-installed the Lumension EMSS server with a different installation directory than the original installation, run the following SQL command.

```
UPDATE SystemConfig SET SystemConfig_Value = 'NewWebInstallPath' WHERE SystemConfig_Name
= 'InstallPath'
```

**30.** Restart the `World Wide Web Publishing Service`, `EDS LanPortal`, `EDS MessageBroker`, `EDS Server`, `Replication Service`, and `STATEngine` services.

**31.** Install the Lumension EMSS Agent from the ***Download Agent Installers*** page.

## Creating an Automated Solution

A Maintenance Plan allows you to create an automated backup and schedule the backup to occur as frequently as your organizational needs dictate. Maintenance Plans allow you to define your back up options as well as which databases and transaction logs to include.

**Note:** If you have not already done so, you should change your Database Recovery Model to `FULL` before continuing. For additional information, refer to *Changing the Database Recovery Model* on page 343.

## Creating a Maintenance Plan

You can automate a database maintenance plan for the SQL Server instances associated with Lumension Endpoint Management and Security Suite.

**Prerequisites:**

Prior to creating a Maintenance Plan you must upgrade your database server to ***Microsoft SQL Server 2008 Standard*** or ***Microsoft SQL Server 2008 Enterprise***, install SSIS (***SQL Server Integration Services***), and set the ***SQL Server Agent*** startup type to `Automatic`.

1. Open the ***Microsoft SQL Server Management Studio*** (**Start** > **Programs** > **Microsoft SQL Server 2008** > **SQL Server Management Studio**).
2. Log into your database server.
3. In the directory tree, expand ***Server Name\SQL Instance*** > **Databases**.
4. Right-click on the **Maintenance Plans** folder.
5. Select **Maintenance Plan Wizard**.

   **Step Result:** The ***SQL Server Maintenance Plan Wizard*** opens.

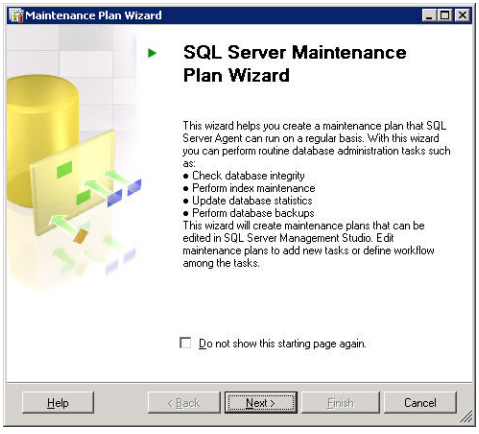

Maintenance Plan Wizard
SQL Server Maintenance Plan Wizard
This wizard helps you create a maintenance plan that SQL Server Agent can run on a regular basis. With this wizard you can perform routine database administration tasks such as:
• Check database integrity
• Perform index maintenance
• Update database statistics
• Perform database backups
This wizard will create maintenance plans that can be edited in SQL Server Management Studio. Edit maintenance plans to add new tasks or define workflow among the tasks.
Do not show this starting page again.
Help
< Back
Next >
Finish
Cancel

Figure 132: SQL Server Maintenance Plan Wizard

6. Click **Next**.

   **Step Result:** The ***Select a Target Server*** page opens.

7. Define the maintenance plan **Name**, **Description** [optional], target **Server**, and **Authentication** method.
8. Click **Next**.

   **Step Result:** The ***Select Maintenance Tasks*** page opens.

9. Select the following maintenance tasks:
   - **Check Database Integrity**
   - **Clean Up History** [optional]

- **Back Up Database (Full)**
- **Back Up Database (Transaction Log)**

10. Click **Next**.

    **Step Result:** The ***Select Maintenance Task Order*** page opens.

11. Set the tasks to execute in the following order:
    - **Check Database Integrity**
    - **Back Up Database (Full)**
    - **Back Up Database (Transaction Log)**
    - **Clean Up History** [optional]
12. Click **Next**.

    **Step Result:** The ***Define Database Check Integrity Task*** page opens.

13. Click the **Database** drop-down.
    a) Select the **These databases** option.
    b) Select the `PLUS`, `PLUS_Staging`, `UPCCommon`, `SCM`, and `STAT_Guardian` databases.
    c) Click **OK**.
14. Ensure that the **Include indexes** option is selected.
15. Click **Next**.

    **Step Result:** The ***Define Back Up Database (Full) Task*** page opens.

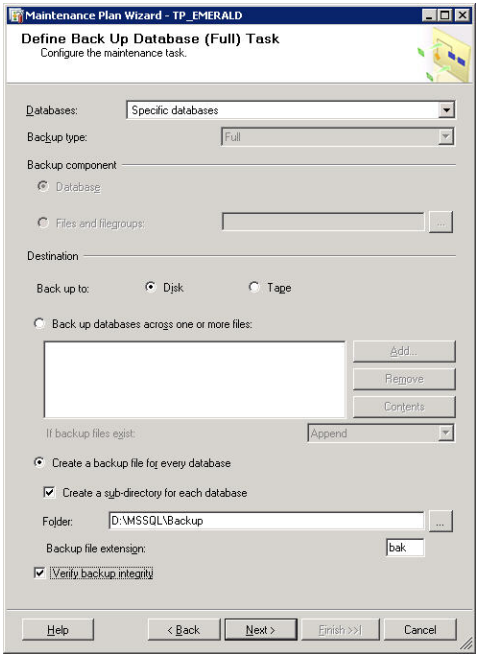



Figure 133: Define Back Up Database (Full) Task

16. Click the **Database** drop-down.
    a) Select the **These databases** option.
    b) Select the `PLUS`, `PLUS_Staging`, `UPCCommon`, `SCM`, and `STAT_Guardian` databases.
    c) Click **OK**.
17. Define your Back up **Destination** settings.
    a) Select either the **Disk** or **Tape** option.
    b) Select to **Create a backup file** for every database.
    c) Select to **Create a sub-directory** for each database.
    d) Define your destination **Folder**.

    **Note:** For performance reasons, it is recommended that you create your database backup in a directory that is not on the same physical drive as your database.

    e) Ensure the **Backup file extension** is set as `bak`.
    f) Select **Verify backup integrity**.
18. Click **Next**.

    **Step Result:** The ***Define Back Up Database (Transaction Log) Task*** page opens.

19. Click the **Database** drop-down.
    a) Select the **These databases** option.
    b) Select the `PLUS`, `PLUS_Staging`, `UPCCommon`, `SCM`, and `STAT_Guardian` databases.
    c) Click **OK**.
20. Define your Back up **Destination** settings.
    a) Select either the **Disk** or **Tape** option.
    b) Select to **Create a backup file** for every database.
    c) Select to **Create a sub-directory** for each database.
    d) Define your destination **Folder**.

    **Note:** For performance reasons, it is recommended that you create your database backup in a directory that is not on the same physical drive as your database.

    e) Ensure the **Backup file extension** is set as `trn`.
    f) Select **Verify backup integrity**.

**21.** Click **Next**.

**Step Result:** If the **Clean Up History** option was selected, the ***Define Cleanup History Task*** page opens. Otherwise the ***Select Plan Properties*** page will open.

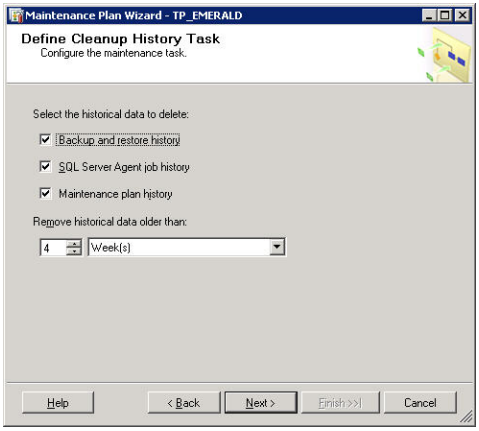



Figure 134: Define Cleanup History Task

**22.** If the **Clean Up History** option was selected, define the ***Cleanup History Task*** options.

a) Ensure that **Backup and restore history** is selected.
b) Ensure that **SQL Server Agent job history** is selected.
c) Ensure that **Maintenance plan history** is selected.
d) Define the **Remove historical data older than** setting as appropriate for your organization.
e) Click **Next**.

**Step Result:** The ***Select Plan Properties*** page will open.

**23.** If desired, click **Change** to open the ***New Job Schedule*** page and define the maintenance plan schedule.

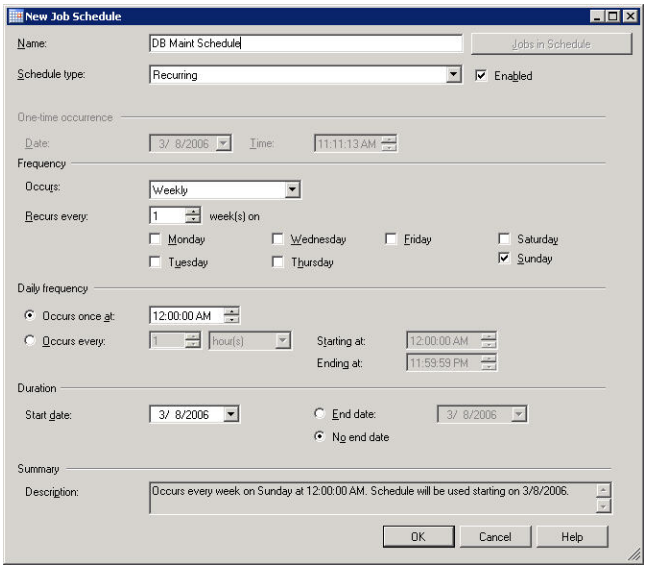



Figure 135: New Job Schedule

a) Enter a **Name** for the schedule.
b) Select a **Schedule** type.
c) Ensure that **Enabled** is selected.
d) Define the **Occurrence** frequency (**Daily**, **Weekly**, or **Monthly**) and options.
e) Define the **Daily frequency**.
f) Define the **Duration**.
g) Click **OK**.

**Step Result:** The changes are saved and the ***New Job Schedule*** page closes.

**24.** Click **Next**.

**Step Result:** The ***Select Report Options*** page opens.

**25.** Set your desired reporting options.

**26.** Click **Next**.

**Step Result:** The ***Complete the Wizard*** page opens.

**27.** Click **Finish** to complete the wizard.

## After Completing This Task:

You must now establish a backup procedure which will archive all of your backup files and the contents of the `UpdateStorage` directory on a regular basis. This can be done through the use of any file backup utility.

# Appendix E

# Installation Manager Reference

**In this appendix:**

- Configuring Windows Firewall for Installation Manager
- Updating Lumension Installation Manager

Within Lumension Endpoint Management and Security Suite, you can use Installation Manager to install Lumension Endpoint Management and Security Suite components.

Under some circumstances, you may need to configure your firewall for communication between Lumension Endpoint Management and Security Suite and Installation Manager. Also, you may need to upgrade Installation Manager itself.

## Configuring Windows Firewall for Installation Manager

Allow Installation Manager to communicate through a Windows Firewall on the Lumension Endpoint Management and Security Suite (Lumension EMSS) server.

**Prerequisites:**

- Install Lumension EMSS.
- An active Firewall is present on the Lumension EMSS server.

Create a port exception through the Firewall for Lumension Installation Manager and Lumension Installation Manager Update.

**Note:** The following steps were created for Windows 2003. When creating a port exception for Windows 2008, steps may differ slightly.

1. Create a port exception through the Firewall.
   a) Click **Start** > **Run**.

b) In the **Open** field, type `firewall.cpl`.

**Step Result:** The ***Windows Firewall*** dialog opens.

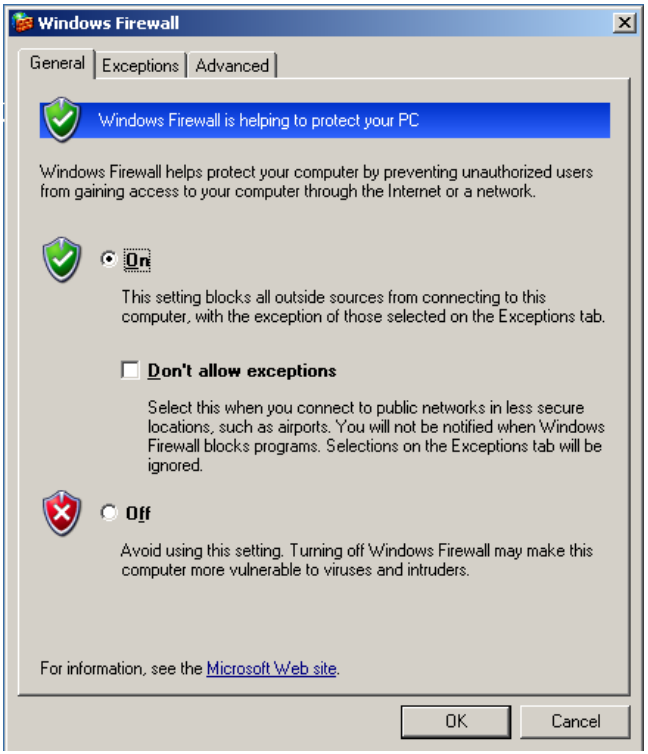

Windows Firewall
General
Exceptions
Advanced
Windows Firewall is helping to protect your PC
Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.
On
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.
Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.
Off
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.
For information, see the Microsoft Web site.
OK
Cancel

Figure 136: Windows Firewall Dialog

c) Click the ***Exceptions*** tab.

d) Click **Add Port**.

**Step Result:** The ***Add a Port*** dialog opens.

e) In the **Name** field, type `Lumension Installation Manager`.

f) In the **Port number** field, type `25745`.

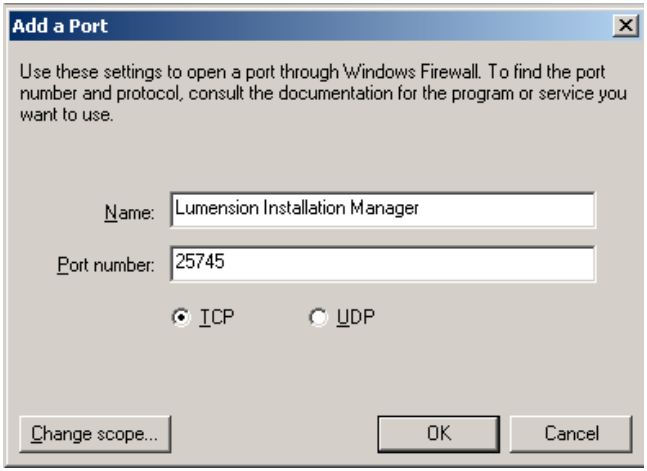

Add a Port
Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.
Name:
Lumension Installation Manager
Port number:
25745
TCP
UDP
Change scope...
OK
Cancel

Figure 137: Add a Port

g) Ensure **TCP** option is selected.
h) Click **OK**.

**Step Result:** The ***Add a Port*** dialog closes.

**2.** Create a port exception through the Firewall for Lumension Installation Manager Update.

a) Click **Add Port**.

**Step Result:** The ***Add a Port*** dialog opens.

b) In the **Name** field, type `Lumension Installation Manager Update`.
c) In the port field, type `25746`.

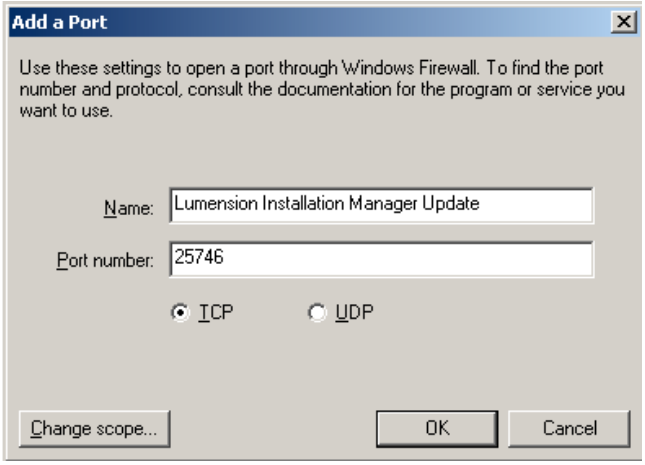

Add a Port
Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.
Name:
Lumension Installation Manager Update
Port number:
25746
TCP
UDP
Change scope...
OK
Cancel

Figure 138: Add a Port

d) Ensure **TCP** option is selected.

e) Click **OK**.

**Step Result:** The ***Add a Port*** dialog closes.

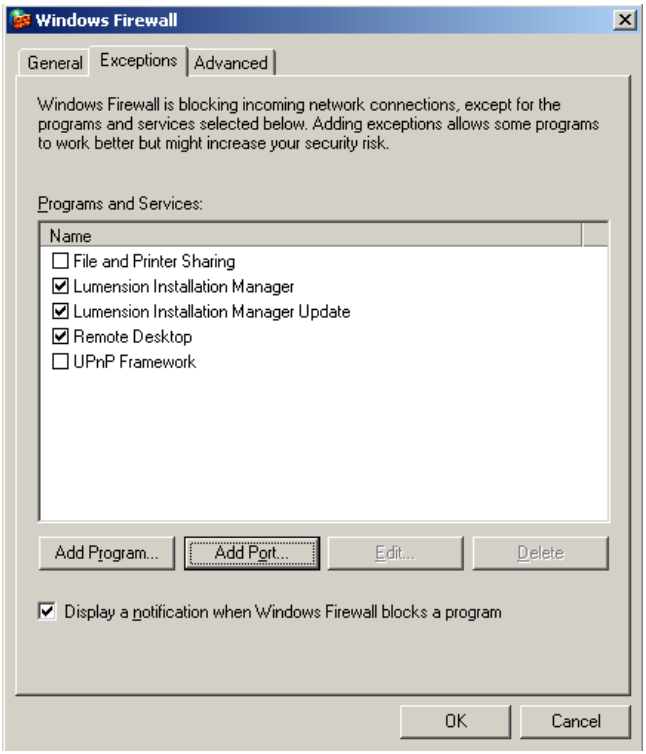



Figure 139: Windows Firewall Dialog

**3.** Click **OK**.

**Step Result:** Closes the ***Windows Firewall*** dialog.

**Result:** The Lumension Installation Manager can communicate through a Windows Firewall on the Lumension EMSS server.

# Updating Lumension Installation Manager

Lumension Installation Manager is updated periodically.

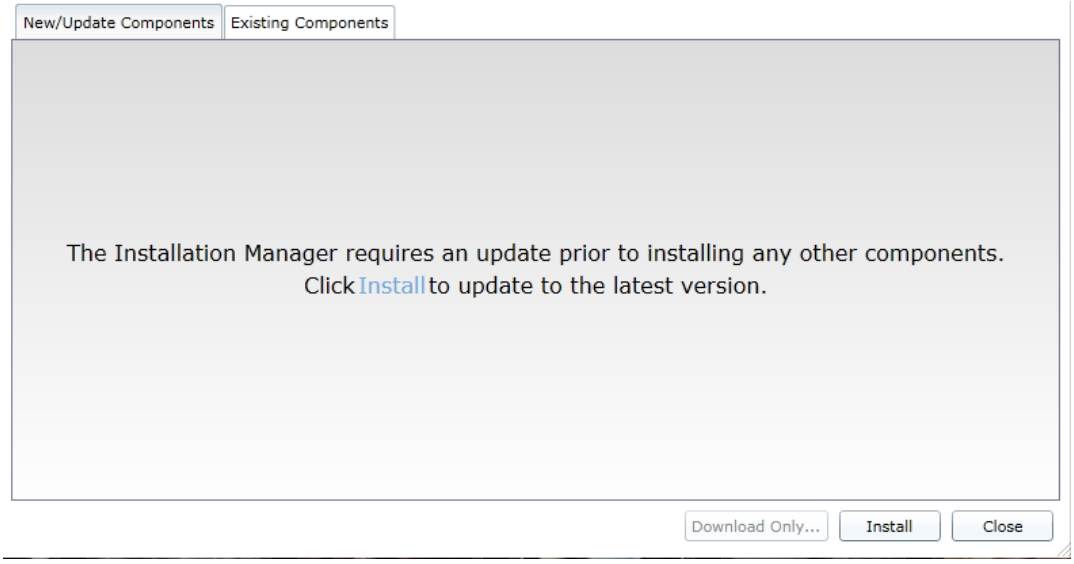

New/Update Components
Existing Components
The Installation Manager requires an update prior to installing any other components.
Click Install to update to the latest version.
Download Only...
Install
Close

Figure 140: New/Update Components Tab

Lumension Installation Manager updates are downloaded and applied by Lumension EMSS, or you can install them manually as any other component. For additional information, refer to *Installing or Updating Components* on page 284. Lumension recommends installing updates immediately.

# Appendix F

# Glossary

**In this appendix:**

- Glossary

This glossary defines terms related to Lumension Endpoint Management and Security Suite. Some terms apply to information technology in general, while others are specific to Lumension Endpoint Management and Security Suite.

## Glossary

This glossary contains list of terms related to Lumension Endpoint Management and Security Suite, as well as their definitions.

### A

| | |
|---|---|
| **AAA Architecture** | In client/server networking, an architecture that combines three necessary elements of security, to make them available on one server and able to work with each other in a coordinated manner. |
| **access control list** | A database file that stores information regarding entities that may request access to a network, as well as the rights and privileges to be granted upon request. |
| **accessible endpoints** | A feature that associates an individual endpoint with a particular role. This feature allows you to limit a user's permissions to specific endpoints. For example, you can limit a user with administrative rights to administration of a single endpoint. |
| **accessible endpoint groups** | A feature that associates an individual group with a particular role. This feature allows you to limit a user's permissions to specific groups. For example, you can limit a user with administrative rights to administration of a single group. |
| **access rights** | System privileges that determine whether or not a user can access an individual feature or page. There is an access right for each system page and function. Access rights for a user are determined by selecting rights for a user role, and then assigning that user role to the applicable user. |

| | |
|---|---|
| **accounting** | In network security architectures, records what users do once they are granted access to a network, or in the case of denied access, it can report how many failed attempts, and even details of the attempts. |
| **ACL** | For additional information, refer to *access control list* on page 363. |
| **Active Directory** | Microsoft's trademarked system that centralizes the management of networked resources by making each item on a network, including most applications, objects in a relational database and then enabling the administrator to manage those objects through one management center. |
| **active directory synchronization** | The process by which the Application Control module synchronizes with a network active directory. This process crawls targeted active directories for users, user groups, endpoints, endpoint containers, and other data stored in the active directory. |
| **Active Server Page** | An HTML page that contains embedded server side scripting that is processed on a Microsoft Web Server before the page is sent to the user. |
| **ActiveX** | A technology, built on Microsoft's Component Object Model (COM), that enables software components, regardless of the language used to create them, to interact with one another in a networked environment. |
| **Active Template Library** | A Microsoft program library for use when creating ASP code and other ActiveX program components to run in a browser window. |
| **AD** | For additional information, refer to *Active Directory* on page 364. |
| **Address Resolution Protocol** | An OSI layer-3 protocol used to find an endpoint's MAC address using its IP address. |
| **agent** | A software routine that resides in background memory on a computer or other device and waits to perform an action when a specified event occurs. |
| **agent management job** | Jobs that let you install agents upon endpoints within your network remotely. The first function of this job is to discover the targeted endpoints as in a discovery scan job. The second function of this job is to install agents upon endpoints discovered during the first function. These jobs access the targeted endpoints by providing credentials specified during job configuration. |
| **agent policies** | The agent rules for communicating with the server. These rules include: communication interval, deployment notification options, discovery agent mode, hours of operation, logging level, and reboot notification options. Agent policies are assigned to groups, but any group that has not been explicitly assigned an agent policy will use the default system policy, as defined within the Lumension Endpoint Management and Security Suite server. |

| | |
|---|---|
| **agent policy conflict resolution** | A series of protocols that determine which setting takes priority when a group or endpoint is assigned two or more agent policy sets with policies that conflict. |
| **agent policy sets** | The combined selected agent policies as defined by the user. After their definition, these sets are then assigned to groups. |
| **ARP** | For additional information, refer to *Address Resolution Protocol* on page 364. |
| **ASP** | For additional information, refer to *Active Server Page* on page 364. |
| **asset** | An endpoint, along with all the hardware and software that is installed on that endpoint. Each endpoint, individual hardware device, and individual software application is considered an asset. |
| **ATL** | For additional information, refer to *Active Template Library* on page 364. |
| **authentication** | The process of identifying a user, typically through the use of credentials such as a user name and password, as the originator of a message or as the end point of a channel. High level authentication can use such other tokens as the originating IP address, or an encryption key, providing evidence of the authenticity of the request. |
| **authentication, authorization, and accounting architecture** | For additional information, refer to *AAA Architecture* on page 363. |
| **Authenticode** | A technology based on information technology security industry standards that provides a method for developers to digitally sign their code. When code is signed, the company signing the code takes responsibility for the code and guarantees that the code is safe and free from viruses. |
| **authorization vs. authentication** | Whereas authentication is the process of verifying that a user is who they say they are, like having two forms of ID from different places, or dating paint and frame wood to verify authenticity of a painting, authorization is verifying the level of access available to that user, such as aisle and row seating stamped on a concert ticket, or possessing a back-stage pass. |
| **authorization** | The process of determining what level of access to grant a user to a system or software application function based upon their log in credentials. |

## B

| | |
|---|---|
| **browser** | Software that allows the user to find, view, hear, and interact with material on a corporate Intranet or the World Wide Web. |

## C

| | |
|---|---|
| **child hierarchy** | The entire group hierarchy belows a specific group within the group hierarchy. Child groups have only one parent. Nesting child groups within parent groups creates an inheritance, which lets you apply one agent policy set to a parent and its children. |
| **client** | In computer networks, a client is any user, computer, node, server, or system that is requesting files from or access to some other system, regardless of whether it also acts as a server. |
| **code signing** | The process of digitally signing programs for verification purposes. |
| **components** | The components that form Lumension Endpoint Management and Security Suite. components come in two types: platform components and module components. Platform components form a basis for module components to operate. Module components are the individual security solutions used to prevent network security breaches. |
| **Component Object Model** | Microsoft's programming architecture in the Windows family of operating systems that enables software components to communicate between processes and fit easily into object-oriented program design. The family of COM technology includes COM+, Distributed COM (DCOM) and ActiveX. |
| **COM** | For additional information, refer to *Component Object Model* on page 366. |
| **context** | Pertaining to Microsoft Active Directory, context refers to the exact container position in the directory tree, thus allowing for the location of resources in a tree, by use of relative rather than fully qualified identifiers. |
| **Control Panel applet** | An application designed to be run within Microsoft Windows Control Panel. Lumension's Control Panel applet allows easy interaction with the Lumension Endpoint Management and Security Suite agent. |
| **Coordinated Universal Time** | An international standard that allows for synchronization of events across many geographic zones. On a Lumension Endpoint Management and Security Suite server, UTC might be chosen instead of local time if a scheduled event is desired to run at the same time at all sites, dependent also upon deployment constraints. |
| **credentials** | An object or objects presented along with a request for admission to a network or server that is used to validate the authorization of the presenter. Usually a credential is a combined user name and password, but can also consist of IP address, MAC address or an encryption key to verify that the request comes form an authorization location. |
| **cross-platform** | Portable or applicable to more than one operating system. |

## D

| | |
|---|---|
| **DCOM** | For additional information, refer to *Distributed Component Object Model* on page 367. |
| **decryption** | The process of converting ciphered text back to plain text after it travels across a public access medium. A previously determined key is used once the text arrives at its destination to convert the ciphered message back to clear text. |
| **decryption key** | A string of seemingly random bits of data used with cryptographic algorithms to create or verify digital signatures and unscramble cipher text back to its original clear text. Keys can be public or private and keeping at least one key private provides high security. Keys at least 128 bits long are considered more secure by modern standards, as many shorter ones have been cracked by modern computing technology. |
| **DHCP** | For additional information, refer to *Dynamic Host Configuration Protocol* on page 368. |
| **directory sync** | For additional information, refer to *active directory synchronization* on page 364. |
| **discovery methods** | The methods used to designate targets (endpoints and devices) during discovery scan jobs. Endpoints and devices can be discovered using a single IP address, an IP address range, a single computer name, network neighborhood, or active directory. |
| **discovery options** | A series of queries and scans that collect information about targets defined for detection during discovery scan jobs. These options (which include Verify with PING, ICMP Discovery, Port Scan Discovery, SNMP Discovery, Windows Version Discovery, Resolve DNS Names, Resolve MAC Addresses, and Resolve NetBIOS Names) identify whether an endpoint is present, and, if one is, what its address and operating system information are. |
| **discovery scan job** | A network-based scan run from the Lumension Endpoint Management and Security Suite server that discovers assets in your network (endpoints, routers, switches, printers, and so on) by using user-specified IP addresses or asset names and/or domains. These jobs also discover additional information about assets (operating system, address information, and so on) through port scans, information queries, and address mask requests. |
| **Distributed Component Object Model** | An extension of the Component Object Model (COM) that extends COM's capabilities across network boundaries, allowing objects to communicate across a network. COM, unlike DCOM, is designed for interprocess communication on the same node or computer. |
| **DLL file** | For additional information, refer to *dynamic-link library file* on page 368. |

| | |
|---|---|
| **DNS** | For additional information, refer to *Domain Name System* on page 368. |
| **domain** | On a local or wide area network, a domain is a set of network resources and services available to a group of users. Domains act as containers that can be identified by a name and address, which can then provide authorized users access to any elements they contain. Domains can also share resources with each other as trust is extended by administrators to those other domains. |
| **Domain Name System** | The system used to name computers and especially servers for easier location. A domain name is a meaningful and human-readable name associated with an IP address. Domain names most often take on the format of domainname.com and the most common ones are associated with WWW locations. |
| **Dynamic Host Configuration Protocol** | A protocol that lets network administrators centrally manage and automate the assignment of IP addresses in an organization's network by establishing a range of IP addresses to be assigned automatically and indexed. Without DHCP, managers would have to manually assign and keep track of each host IP address on the network. |
| **dynamic-link library file** | A file that has linked and compiled one or more functions used by a separate process, which can be loaded into the memory space of that process when the program is started or running. |

## E

| | |
|---|---|
| **encryption** | The process of converting clear, readable text to ciphered text before it travels on network media, so that it can only be read or understood by a recipient with the proper decryption key. Some of the most secure encryption methods include RSA, AES, IKE, MDS, SSL, and SHA-1. |
| **encryption key** | A string of ciphered bits used with cryptographic algorithms to create or verify digital signatures and scramble clear text to protect it from being intercepted and read while traveling across public networking media. Keys can be public or private, and keeping at least one key private provides high security. Keys at least 128-bits long are considered more secure by modern standards, as many shorter ones have been compromised by modern computing technology. |
| **endpoint** | In a client/server network architecture, an endpoint is any node that is a destination of two-way communication, whether requesting or responding. Additionally, in regard to the Lumension Endpoint Management and Security Suite, the term endpoint is synonymous with any computer in your network that can have an agent installed. |
| **extensible markup language (XML)** | For additional information, refer to *XML* on page 377. |

## F

| | |
|---|---|
| **File Transfer Protocol** | A protocol that uses simple, clear text. Thus, it is a non-secure protocol used to exchange files between computers on a network or the internet. |
| **firewall** | A firewall is a set of related programs located at a network gateway server that protects the resources of a private network from unauthorized access. |
| **FQDN** | For additional information, refer to *fully qualified domain name* on page 369. |
| **FTP** | For additional information, refer to *File Transfer Protocol* on page 369. |
| **fully qualified domain name** | The domain name is a unique identifier for any resource located within a domain or network. A FQDN is the full name of any network entity starting with its hostname and ending with the exact domain name in which it resides. Example: johnq.accounting.acme.com |

## G

| | |
|---|---|
| **globally unique identifier** | A 128-bit number generated by Windows operating systems or one of its applications, which is assigned to any object in a two-way communication, be it user, application, or component. The algorithm used to generate GUIDs combines a few unique settings, such as IP Address, MAC Address, and clock date and time to create an even more unique identifier. |
| **group** | A targeted collection of computers created and named for the purpose of deploying distribution packages, defining agent policies, setting Mandatory Baselines, or reporting. Groups provide a simple way to manage computers that have similar requirements rather than managing each computer separately. |
| **GUID** | For additional information, refer to *globally unique identifier* on page 369. |

## H

| | |
|---|---|
| **hostname** | The name given to identify each node of a network. The hostname usually describes either the user that operates the node, its position in a building, or its function. Hostname is intended to be more human friendly than numeric IP Addresses. |
| **HTML** | The accepted publishing language of the World Wide Web. It is a universally accepted standard for displaying links, images, and text in a format that computers around the world can read. There are currently many advantages in HTML that allow for an increasing number of different types of objects to be added to and displayed in a browser page. |
| **HTTP** | The set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. |

| | |
|---|---|
| **HTTPS** | A Web protocol built into most browsers that encrypts and decrypts user page requests as well as the pages that are returned via HTTP over SSL by the Web server. |
| **hyperlink** | Generally a different color from the surrounding text, a hyperlink is a coded reference to another location in the document, or to a URL or network address, usually written in a form of HTML code or JAVA, and is most prevalent on Web pages. |
| **HyperText Markup Language** | For additional information, refer to *HTML* on page 369. |
| **HyperText Transfer Protocol** | For additional information, refer to *HTTP* on page 369. |

## I

| | |
|---|---|
| **IANA** | For additional information, refer to *Internet Assigned Numbers Authority* on page 370. |
| **IIS** | For additional information, refer to *Internet Information Services* on page 370. |
| **Internet Assigned Numbers Authority** | An administrative organization that assigns internet host addresses and other numeric constants used in Internet protocols. |
| **Internet Information Services** | Microsoft's Web server that provides an infrastructure for all Internet services (HTTP, FTP, Telnet, and Gopher for some examples) and other capabilities for Microsoft's NT, XP, 2000, 2003, 2008, and Vista operating systems. The IIS Manager allows for central control of all related information services. |
| **Internet Protocol** | For additional information, refer to *IP* on page 370. |
| **IP** | The best known and main protocol in a suite of protocols known as TCP/IP that carry all traffic on the internet currently. IP is a connectionless protocol, meaning it does not wait for confirmation that it was received before sending the next packet. It is designed for long distance carriage of packets of data, as was originally the plan with Arpanet, which later became the internet. |
| **IP address** | The 32-bit (4 dotted divisions of eight binary digits) numeric identifier for any device on a network that distinguishes it from other devices and allows for routers and switches to group devices and their communication packets. The 32-bit dotted format is soon to be replaced by IPv6, which will expand the number of available IP addresses to keep pace with the enormous growth of the internet in recent years. Example: IP address 192.168.0.1 would be read by a router as 11000000.10101000.00000000.00000001. |

## J

| | |
|---|---|
| **JAVA** | A programming language invented by Sun Microsystems. It can be used as a general purpose application programming language with built-in networking libraries. It can also be used to write small applications called applets. |
| **JAVA Runtime Environment** | Created by Sun Microsystems, it is the core set of files necessary to execute JAVA written programs in any OS environment. JAVA is used because it is cross-platform, which is increasingly necessary in the current Web-based world. |
| **JRE** | For additional information, refer to *JAVA Runtime Environment* on page 371. |

## L

| | |
|---|---|
| **LDAP** | For additional information, refer to *Lightweight Directory Access Protocol* on page 371. |
| **library** | A collection of precompiled routines, sometimes called modules, that are stored in object format for reuse by a program. |
| **Lightweight Directory Access Protocol** | A software protocol that enables the use of Directory Services to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet. |
| **localhost** | The default name describing the computer address also known as the loopback address of the computer. On Web servers, this loopback can be used to test the default Web page. To access this page, type http://127.0.0.1 or http://localhost. |
| **localprofile.txt** | An XML file found in the C:\ProgramFiles\Lumension\Patch Agent, this file is maintained by the Lumension Endpoint Management and Security Suite agent and contains information on computer's name, services, software, hardware, operating system, and support pack level. The refresh inventory data system task uses the information in this file to populate computer inventory data on the Lumension Endpoint Management and Security Suite server. |
| **Lumension Content Wizard** | Lumension Content Wizard (LCW). An addition to Lumension Endpoint Management and Security Suite that provides the ability to define custom detection reports, deployment packages, signatures, and fingerprints. It has an easy-to-use graphical interface that illustrates all associated subcomponents of the patch in a single view. |

| | |
|---|---|
| **Lumension Endpoint Management and Security Suite** | An application that serves as a platform for other applications that protect your network from security risks. These applications, called *modules*, use different approaches to protect your endpoint. Lumension EMSS is composed of a server component and an agent component. The server component is installed on a server within your network. The agent component is installed on network endpoints you want to protect from security risks. Lumension EMSS is accessed via a Web UI. |
| **Lumension Endpoint Management and Security Suite administrator** | Any user who is assigned any of the access rights that control the functionality of the Lumension Endpoint Management and Security Suite server or its deployments is considered a Lumension Endpoint Management and Security Suite administrator. |
| **Lumension Endpoint Management and Security Suite Agent** | Lumension Endpoint Management and Security Suite Agent. The Lumension Endpoint Management and Security Suite agent is a service that runs on each node and queries the Lumension Endpoint Management and Security Suite server to receive any deployments that become ready. The behavior of the agent is defined by the agent's policies, whether it is using the default agent policies of the Lumension Endpoint Management and Security Suite server or the group's agent policies. |
| **Lumension Endpoint Management and Security Suite Server** | Lumension Endpoint Management and Security Suite. The central system in Lumension Endpoint Management and Security Suite that manages content retrieval, vulnerability detection, and package deployment to all registered computers on the network. As a sophisticated, automated central repository of the most current security content available for a network, it maintains communication with the Lumension Endpoint Management and Security Suite agent on nodes, across many key networking platforms, on the network, and detects any vulnerabilities with the help of the agent on each node. |
| **Lumension Endpoint Management and Security Suite user** | Any user who has access to authenticate in to the Lumension Endpoint Management and Security Suite server is considered a Lumension Endpoint Management and Security Suite user. |

## M

| | |
|---|---|
| **MAC address** | A 12-digit hexadecimal address that is burned into network cards and networking devices to allow for unique reference. |
| **macro** | Within Lumension Endpoint Management and Security Suite, a macro is an environment variable that represents a filename, directory path, or a series of commands, actions, or keystrokes that can only be executed by the Lumension Endpoint Management and Security Suite agent. |

| | |
|---|---|
| **Microsoft SQL Desktop Edition** | An enabling technology that provides local data storage and is completely compatible with the SQL Server version 7.0 code base. This technology transforms Microsoft Access from a simple file-server database application into an extremely powerful and highly scalable client-server solution for any size organization. |
| **Module Components** | Individual security solutions used to prevent various types of security breaches within your network. Each module plugs in to the Lumension EMSS platform and can be purchased individually. Some module components come installed with the Lumension EMSS platform and require no additional licensing. |
| **Module Sub Components** | The two parts that form a module component. Each module component consists of a server sub component and an endpoint subcomponent. These subcomponents work together to form a module's functionality. |
| **MSDE** | For additional information, refer to *Microsoft SQL Desktop Edition* on page 373. |
| **MSI installer** | Designed for Windows networks that use the Windows software installer mechanism. The MSI installer can be edited to include the Lumension Endpoint Management and Security Suite server name and serial number. In this way, the agent can be deployed through the use of group policy agents. |

## N

| | |
|---|---|
| **NDS** | For additional information, refer to *Novell Directory Services* on page 373. |
| **NetWare** | Networking OS that has played a major role in the development of Local Area Networking over the past few decades, being an early Network OS to use the Directory Services concept. |
| **Novell Directory Services** | The relational database that contains all the resources on a Novell network, and provides security, and access for all resources. |

## O

| | |
|---|---|
| **Open Software Description** | Creates a standard way to describe software components, their versions, underlying structure and relationships to other components. OSD is the standard language used when performing automatic software distributions and updates over the Internet. |
| **Operating System Pack** | Contains all vulnerability detection information needed by an agent for a given operating system. It is generated by the DS and is passed to the agent during the DAU task. When a vulnerability replication executes, it checks to see if any operating systems received new data and it will automatically schedule the DS to regenerate the OS Packs for those operating systems. |

| | |
|---|---|
| **OSD** | For additional information, refer to *Open Software Description* on page 373. |
| **OS Pack** | For additional information, refer to *Operating System Pack* on page 373. |
| **P** | |
| **parent hierarchy** | Refers to the entire group hierarchy above a specific group within the group hierarchy. |
| **platform components** | The essential components needed for Lumension Endpoint Management and Security Suite operation. These components include the Lumension EMSS Web console, the Lumension EMSS database, and the Lumension Installation Manager. |
| **policies** | For additional information, refer to *agent policies* on page 364. |
| **policy server** | In a network designed with protections against unauthorized admission, it is where the rules and policies are stored that are the standards by which admission decisions are made. Rules can then be enforced by routers or some other form of firewall protection. |
| **port number** | The port number is carried in internet transport protocols to identify which service or program is to receive an incoming packet. Certain port numbers are permanently assigned to particular protocols by the IANA. For example, e-mail uses port 25 and Web services use port 80. |
| **proxy server** | In an enterprise that uses one of the Internet protocols, a proxy server is a server that acts as an intermediary between a client and an Internet server. The proxy server allows an enterprise to ensure security and administrative control. |
| **Q** | |
| **Q-chain (QChain.exe)** | The utility Microsoft provides to chain hotfixes on Microsoft Windows NT, 2000, 2003, 2008, XP, or Vista. |
| **R** | |
| **Refresh Inventory Data** | Prevents certain log files from getting too large. RID is handled differently on the various platforms; some delete the files when they reach a certain size, while others will trim the file, leaving the most recent data but shrinking the file size. |
| **registry** | The registry serves as a central data repository for system and application-specific configuration data on a Windows machine. A registry contains keys, which are like directories in a Windows file system. Each key can contain values (the registry equivalent of a data file) or nested subkeys (the registry equivalent of a nested folder). Just as with files or folders, you can identify a registry key by building a full path to it. |

| | |
|---|---|
| **replication** | The process whereby the Lumension Endpoint Management and Security Suite server receives daily scheduled updates of patches from the GSS. The schedule replication time of day can be manually overridden daily by clicking **Update Now**. |
| **report** | Records that document activity and information pertaining to your network environment. Within the Lumension Endpoint Management and Security Suite server, you can generate reports for virtually every function that the server and agent performs: endpoint inventory, the results of discovery scan jobs, the status of a deployment, and so on. |
| **Reverse Address Resolution Protocol (RARP)** | Literally, the reverse of Address Resolution Protocol, RARP resolves an IP address from a given hardware, or MAC address. |
| **RID** | For additional information, refer to *Refresh Inventory Data* on page 374. |
| **role** | A group of access rights, accessible groups, and accessible endpoints that can be assigned to users. Roles come in two varieties: system roles and custom roles. System roles are basic groupings of common access rights that come with the Lumension Endpoint Management and Security Suite server and can access all groups and endpoints. These roles include Administrator, Manager, Operator, and Guest. Custom roles are user-created roles that can be edited to fit the needs of individual enterprises; you can fine tune them to add or delete certain access rights. |
| **rules** | Statements of conditions that must be met or parameters that will determine an action to be taken. Rules can be positive or negative, but usually are stated simply and clearly such as “if member of group ADMIN, run superuser.bat.” |

## S

| | |
|---|---|
| **Secure File Transfer Protocol** | A secure version of FTP, SFTP is designed to provide some encryption capabilities for file transfer over a network. Functionally similar to FTP, SFTP instead uses SSH to transfer files, so it cannot be used with a standard FTP client. |
| **Secure HyperText Transfer Protocol** | For additional information, refer to *HTTPS* on page 370. |
| **Secure Sockets Layer** | A security protocol that provides data encryption, message integrity, and client/server authentication for the transmission of private information and documents over the internet. SSL is available with either 40-bit or 128-bit encryption. However, 40-bit has been compromised in recent years, making 128-bit the lowest level anyone should go for secure encryption. |
| **server** | A server is a computer or software application that provides data to client computers or software applications. A single computer running multiple software applications can simultaneously perform the function of multiple servers, multiple clients, or any combination thereof. |

| | |
|---|---|
| **SFTP** | For additional information, refer to *Secure File Transfer Protocol* on page 375. |
| **source group** | Groups that automatically assigned managed endpoints to associated custom groups. |
| **SQL** | For additional information, refer to *structured query language* on page 376. |
| **SQL Server** | A trademark for a Microsoft database server that uses SQL. SQL Server is a popular database management system for Windows NT environments. |
| **SSL** | For additional information, refer to *Secure Sockets Layer* on page 375. |
| **structured query language** | A database language used by administrators of relational databases to query, update, and mange data. It enables the administrator to use clear syntax that is descriptive of whatever action is wanted. |
| **SSL Certificate** | An electronic certificate consisting of a set of keys, one public, one private, exchanged between a Web server and a requesting client. A session is created, and a unique session key ensures a high level of encryption of any sensitive data passed between the client and server, preventing interception or unauthorized use of that data by any other entity. |

**T**

| | |
|---|---|
| **TCP/IP** | The main suite of communications protocols used to connect hosts on the Internet, and now the prevalent LAN protocol even when other protocols are available. |
| **transaction log** | A Web server file that records a history of actions such as data changes. This log is used to roll the Web server back to a stable condition should the database be found in an inconsistent state. |
| **Transmission Control Protocol/ Internet Protocol** | For additional information, refer to *TCP/IP* on page 376. |
| **trust** | In domains, a trust relationship will allow members of one domain, when properly logged in and authenticated, to access services available on another domain. |

**U**

| | |
|---|---|
| **UDP** | For additional information, refer to *User Datagram Protocol* on page 377. |
| **Universal Resource Locater** | For additional information, refer to *URL* on page 376. |
| **URL** | The address that is the formal access name for a network or Internet resource. It usually begins with the protocol identifier, such as http or ftp. Thus, http://www.yahoo.com is a URL for the domain yahoo.com. |

| | |
|---|---|
| **user** | A profile used to access the Lumension Endpoint Management and Security Suite server. These profiles include credentials (a user name and password) and an assigned role that determines the user's access rights within the system. |
| **User Datagram Protocol** | A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses *Internet Protocol*. It is one of the most common connection based protocols in use on the internet, the other being TCP. |
| **user name** | The unique name used to gain access to a computer and/or network. User names and passwords are required in multi-user systems. |
| **user role** | See *role* on page 375. |
| **UTC** | For additional information, refer to *Coordinated Universal Time* on page 366. |

## V

| | |
|---|---|
| **VeriSign certificate** | A VeriSign certificate is issued by VeriSign, Inc. to verify a company's identity and enables the company to digitally sign programs and prove the authenticity of a Web site address. |

## W - Z

| | |
|---|---|
| **Web server** | A program that publishes content using the HTTP protocol so that it can be viewed using any type of compliant browser from any location on the connected Intranet or Internet. |
| **widget** | A graph or chart displayed on the Lumension Endpoint Management and Security Suite ***Home*** page that depicts Lumension Endpoint Management and Security Suite and Lumension Endpoint Management and Security Suite module activities. |
| **World Wide Web (WWW)** | A commonly used name for the Internet, the WWW is a Web of connected Domains of local computers, which can share information with authorized users whom connect from anywhere else on the Web. Due to the exponential growth in recent years, a good way to check on current standards is to visit the *World Wide Web Consortium* (*http://www.w3.org*). |
| **XML** | A flexible way to create common information formats and share both the format and the data on the World Wide Web, Intranets, and elsewhere. |